MODERN DATA NETWORKS

Dr. Sundar Singh
Neeraj Kaushik

Modern Data Networks

Modern Data Networks

Dr. Sundar Singh
Neeraj Kaushik

BOOKS ARCADE
KRISHNA NAGAR, DELHI

Modern Data Networks

Dr. Sundar Singh
Neeraj Kaushik

BOOKS ARCADE

Regd. Office:
F-10/24, East Krishna Nagar, Near Vijay Chowk, Delhi-110051
Ph. No: +91-11-79669196, +91-9899073222
E-mail: info@booksarcade.co.in, booksarcade.pub@gmail.com
Website: www.booksarcade.co.in

Year of Publication 2023

International Standard Book Number-13: 978-81-19199-70-9

CONTENTS

Chapter 1 Efficient Data Communication: Strategies for Optimizing Bandwidth Utilization and Minimizing Latency in Modern Networks 1

—Dr. Sundar Singh

Chapter 2 Interconnecting Networks: A Review of Topologies, Protocols, and Emerging Technologies for Scalable and Reliable Communication 8

—Dr. Pooja Sagar

Chapter 3 Analysis and Comparison of Network Models: A Comprehensive Study on Graph Theory, Machine Learning, and Statistical Approaches for Network Analysis 16

—Dr. Lokesh Kumar

Chapter 4 TCP/IP Protocol Suite: An Overview and Analysis of the Most Widely Used Internet Protocol Stack in the World 25

—Dr. Himanshu Singh

Chapter 5 Physical Layer and Media: An Analysis of the Fundamentals, Challenges, and Advancements in Data Communication Technologies 32

—Dr. Deepak Chauhan

Chapter 6 Data and Signals: A Comprehensive Study on the Fundamentals and Applications of Digital Communication 41

—Dr. Narendra Kumar Sharma

Chapter 7 Digital Transmission: A Comparative Study on Modulation Techniques and Channel Coding for Reliable and Efficient Communication 49

—Dr. Abhishek Kumar Sharma

Chapter 8 Signal Encoding Techniques: A Comprehensive Analysis of Encoding Schemes for Efficient and Secure Digital Communication 59

—Dr. Govind Singh

Chapter 9 Digital Data Communication Techniques: A Comparative Analysis of Modulation, Multiplexing, and Coding Techniques for High-Speed and Reliable Communication 68

—Dr. Arvind Kumar Pal

Chapter 10 Analog Transmission: Challenges and Advancements in Analog Communication Systems for Robust and Efficient Communication 75

—Dr. Deepanshu Singh

Chapter 11 Bandwidth Utilization: A Comparative Study of Multiplexing and Spreading Techniques for Efficient and Secure Data Transmission 83

—Neeraj Kaushik

Chapter 12 Transmission Media: A Comprehensive Analysis of Wired and Wireless Communication Channels for Modern Data Communication Systems 93

—Prashant Kumar

Chapter 13 Switching: A Review of Circuit, Packet, and Message Switching Techniques for Efficient and Scalable Data Communication Networks 102

—Rahul Vishnoi

Chapter 14 Datagram Networks: An Analysis of Datagram Packet Switching Techniques for Reliable and Efficient Data Communication 109

—Pankaj Kumar Goswami

Chapter 15 Using Telephone and Cable Networks for Data Transmission: A Comparative Analysis of DSL and Cable Modem Technologies for High-Speed and Reliable Data Communication 116

—Rahul Sharma

Chapter 16 Data Link Layer Error Detection: A Comparative Study on Hamming, and Parity Check Techniques for Robust and Reliable Data Communication 123

—Alka Verma

Chapter 17 Analysis and Comparison of Data Link Control Protocols for Reliable Data Transfer in Communication Networks 130

—Neeraj Kaushik

Chapter 18 Performance Evaluation of Data Link Control Protocols for Efficient Data Transfer in Communication Networks 139

—Prashant Kumar

Chapter 19 Design and Implementation of a Robust Data Link Control Protocol for High-Speed Communication Networks 148

—Rahul Vishnoi

Chapter 20 Multiplexing Techniques for Efficient Data Transmission: A Comprehensive Review 157

—Pankaj Kumar Goswami

Chapter 21 Spread Spectrum: A Comprehensive Study on Theory, Techniques, and Applications for Secure and Efficient Data Communication 165

—Rahul Sharma

Chapter 22 Circuit Switching and Packet Switching: A Comparative Analysis of Techniques for Reliable and Efficient Data Communication Networks 173

—Alka Verma

Chapter 23 Asynchronous Transfer Mode (ATM): Architecture, Protocols, and Applications in Modern Communication Networks 182

—Prashant Kumar

Chapter 24 Efficient Routing Strategies for Switched Networks: A Comparative Study of Traditional and Modern Approaches 192

—Pankaj Kumar Goswami

CHAPTER 1

EFFICIENT DATA COMMUNICATION: STRATEGIES FOR OPTIMIZING BANDWIDTH UTILIZATION AND MINIMIZING LATENCY IN MODERN NETWORKS

Dr. Sundar Singh, Assistant Professor,
Department of Computer Science, Sanskriti University, Mathura, Uttar Pradesh, India,
Email id- sundar@sanskriti.edu.in

ABSTRACT:

Data communications is the process of transmitting digital information between two or more devices or computers over a communication medium. It involves the use of a variety of techniques and technologies to facilitate the exchange of data and ensure that it is transmitted reliably and securely. The process of data communication can be divided into several layers, each of which is responsible for a specific aspect of the transmission. These layers include the physical layer, which deals with the physical transmission of data, the data link layer, which provides error detection and correction, the network layer, which manages the routing of data, and the application layer, which provides the interface between the user and the network.

KEYWORDS:

Communication, Data, Physical Layers, Link Layers, Technologies.

INTRODUCTION

Data communication involves the use of various techniques and technologies to facilitate the exchange of data and ensure that it is transmitted reliably and securely. These techniques include modulation, multiplexing, routing, error detection, and correction. Each of these techniques plays a specific role in the data communication process [1]–[3].The process of data communication can be divided into several layers, each of which is responsible for a specific aspect of the transmission. These layers include the physical layer, data link layer, network layer, transport layer, session layer, presentation layer, and application layer. The physical layer deals with the physical transmission of data, while the data link layer provides error detection and correction. The network layer manages the routing of data, and the transport layer ensures that data is delivered reliably and in the correct order.

The session layer establishes and maintains communication sessions between devices. The presentation layer translates data between the application and network layers, and the application layer provides the interface between the user and the network. Data communications can be conducted using a variety of media, including wired and wireless connections. Wired connections include Ethernet, coaxial cables, and fiber optic cables, while wireless connections include Wi-Fi, Bluetooth, and cellular networks. The choice of medium depends on factors such as the distance between devices, the speed of the transmission, and the need for security.

One of the significant advantages of data communication is the speed at which data can be transmitted [4]. With the advent of high-speed internet, data can be sent and received almost instantaneously, no matter where the sender or receiver is located. This has had a profound

impact on business, allowing companies to communicate with customers and suppliers quickly and efficiently. It has also revolutionized the way people communicate with one another, enabling people to stay in touch with friends and family, no matter where they are located.

Another significant advantage of data communication is its ability to handle large volumes of data. With the growth of big data, data communication has become more critical than ever, enabling organizations to analyze vast amounts of data to gain insights and make informed decisions [5]. This has revolutionized the way companies do business, allowing them to identify trends and patterns in customer behavior, track sales and inventory, and optimize supply chain operations.Data communication has also led to the growth of e-commerce, enabling companies to sell products and services online. Online shopping has become increasingly popular, and it has become the preferred way of shopping for many people. E-commerce has also made it easier for companies to reach a global audience, enabling them to sell products and services to customers anywhere in the world.

However, data communication is not without its challenges. One of the significant challenges is security [6], [7]. With the growth of online transactions, there has been a corresponding increase in cybercrime, with hackers attempting to steal sensitive data such as credit card numbers, social security numbers, and other personal information. This has led to the need for strong security measures such as encryption and firewalls to protect data from unauthorized access.Another challenge is the need to ensure that data is transmitted reliably and in the correct order. This is particularly important for real-time applications such as video conferencing and online gaming, where delays and lost data can have a significant impact on the user experience.

DISCUSSION

We exchange information when we talk to one another. Local or distant sharing are both possible. Local communication takes place face-to-face between people, while distant communication happens over space. The phrase "telecommunication" refers to long-distance communication (telephony), telegraphy, and television. Information delivered in any format that is accepted by the people that are generating and consuming the data is referred to as data [8], [9]. Data communications are the transfer of data between two devices via a wire connection or other kind of transmission media. The communicating devices must be a part of a communication system composed of a mix of hardware (physical equipment) and software for data communications to take place (programs). Delivery, accuracy, timeliness, and jitter are the four key qualities that determine how well a data communications system performs. Data delivery to the proper location must be ensured by the system. The designated device or user must get the data, and only that device or user.

The data must be correctly sent by the system. Data that has been tampered with during transmission and is not restored is useless. Data must be sent by the system promptly. Late data delivery is meaningless. When it comes to video and audio, timely delivery entails sending the data as soon as it is created, in the same sequence, and without any noticeable delays. Real-time transmission is the term for this kind of distribution. The term "jitter" describes the variance in packet arrival times. It is the unequal delay in audio or video packet transmission. For example, suppose that video packets are transmitted every 3D milliseconds. Uneven video quality results if some packets arrive with a 3D-ms delay while others arrive with a 4D-ms delay. The information (data) that has to be transmitted is the message. Information in the form of text, numbers, images, music, and video is quite common. The data message's sender is the sending device. It could be a

computer, workstation, phone, video camera, or other device. The device that receives the message is called the receiver. It could be a computer, workstation, phone, television, or another device.Transmission medium, item one. The physical route used by a message as it travels from sender to receiver is known as the transmission medium. Twisted-pair wire, coaxial cable, fiber-optic cable, and radio waves are a few types of transmission medium. Data transmission is governed by a set of rules known as a protocol. It stands for a compromise between the communicators. Without a protocol, two devices can be linked but unable to communicate, much as someone speaking Japanese and French cannot understand one other.

Nowadays, information is available in a variety of formats, including text, numbers, photos, audio, and video. Text is represented as a bit pattern, or a series of bits, in data transfers. To represent text symbols, many bit pattern sets have been developed. Coding is the process of representing symbols, and each set is referred to as a code. Unicode, the current standard coding system, employs 32 bits to represent every symbol or letter used in any language in the world. The first 127 characters of Unicode, generally known as Basic Latin, are made up of the American Standard Code for Information Interchange (ASCII), which was created in the United States many years ago. Bit patterns may also be used to represent numbers. To make mathematical processes simpler, a number is immediately transformed to a binary number rather than being represented by a code like ASCII. A variety of distinct numbering schemes [10].

Bit patterns may also be used to represent images. An image is made up of a matrix of pixels, or "picture components," where each pixel is a tiny dot. The resolution affects how big a pixel is. A picture may be split, for instance, into 1000 or 10,000 pixels. More resolution and a better representation of the picture are present in the second scenario, but more memory is required to retain the image. Each pixel is given a bit pattern after being separated into individual pixels in a picture. The picture determines the pattern's size and value. I-bit pattern is sufficient to represent a pixel for an image made up entirely of black and white dots (such as a checkerboard). You may expand the bit pattern to incorporate grey scale if a picture doesn't consist entirely of pure white and pure black pixels. Use 2-bit patterns, for instance, to display grayscale on four different levels. A black pixel may be represented by the numbers 00, 01, 10, and 11, whereas a light grey pixel can be represented by the number 10.

Color picture representation may be done in a number of ways. A technique is known as RGB since it combines the three main hues of red, green, and blue to create each color. Each color's intensity is quantified, and a bit pattern is then allocated to it. A different technique is known as YCM, in which a color is created by mixing three more primary colors: yellow, cyan, and magenta. The recording or transmission of sound or music is referred to as audio. Audio differs from text, numbers, and visuals by its very nature. It is not distinct; it is continuous. Even when we use a microphone to convert speech or music to an electric signal, we still produce a continuous signal learn how to convert sound or music to a digital or analogue stream.

An image or movie that has been recorded or aired is referred to as video. Video may be created as a single continuous entity (for example, by a TV camera) or as a collection of discrete pictures combined to create the illusion of motion. Data communication refers to the transfer of digital data between devices or computers over a network. It is a fundamental aspect of modern communication and plays a crucial role in how businesses and individuals interact and share information. This article will explore the various components of data communication, including the types of data communication, communication channels, protocols, and standards.

Types of Data Communication

There are two main types of data communication: analog and digital. Analog communication involves sending signals that vary continuously in amplitude, frequency, or phase. Examples of analog communication include telephony, radio broadcasting, and television transmission. In contrast, digital communication involves encoding information in discrete symbols or bits. Digital communication is more efficient and less prone to errors compared to analog communication.

Communication Channels

A communication channel is the medium through which data is transmitted between devices. There are three main types of communication channels: guided, unguided, and wireless. Guided communication channels are those that use physical cabling or wiring to transmit data. Examples of guided communication channels include twisted-pair cables, coaxial cables, and fiber-optic cables. Twisted-pair cables are the most commonly used type of guided communication channel and are used in local area networks (LANs) and telephone systems. Coaxial cables are used in cable television and high-speed internet connections. Fiber-optic cables are used in high-speed internet connections and long-distance communication.

Unguided communication channels are those that use the air as the transmission medium. Examples of unguided communication channels include radio and satellite communication. Radio communication involves transmitting signals over the air using antennas, while satellite communication involves transmitting signals to and from satellites in orbit. Wireless communication channels use wireless technologies such as Wi-Fi, Bluetooth, and cellular networks to transmit data. Wi-Fi is used to create wireless LANs, while Bluetooth is used to connect devices such as smartphones, tablets, and headphones. Cellular networks are used to provide wireless connectivity to mobile devices such as smartphones and tablets.

Protocols

A protocol is a set of rules and standards that govern how data is transmitted over a network. Protocols ensure that data is transmitted in a reliable and secure manner and that the receiving device can correctly interpret the data. There are several types of protocols, including transmission control protocol/Internet protocol (TCP/IP), file transfer protocol (FTP), hypertext transfer protocol (HTTP), and simple mail transfer protocol (SMTP). TCP/IP is the most widely used protocol in the world and is used for transmitting data over the internet. FTP is used for transferring files over the internet, while HTTP is used for transmitting web pages and other internet content. SMTP is used for sending and receiving email.

Standards

Standards are a set of guidelines and specifications that ensure that devices and networks can interoperate with each other. Standards ensure that devices from different manufacturers can communicate with each other and that networks can interoperate seamlessly. There are several organizations that develop and maintain standards for data communication. The Institute of Electrical and Electronics Engineers (IEEE) is one such organization and is responsible for developing standards for LANs and wireless networks. The International Organization for Standardization (ISO) is another organization that develops standards for data communication and is responsible for the development of the OSI model.

The OSI Model

The OSI (Open Systems Interconnection) model is a framework that describes how data is transmitted over a network. The OSI model consists of seven layers, each of which has a specific function in the data communication process. One of the significant trends in data communication is the growth of the Internet of Things (IOT). The IOT refers to the interconnected network of devices that are embedded with sensors, software, and other technologies that enable them to collect and exchange data. The growth of the IOT has the potential to revolutionize industries such as healthcare, transportation, and manufacturing, enabling companies to optimize operations, reduce costs, and improve the customer experience.

Another trend is the growth of 5G networks, which are expected to offer faster speeds, lower latency, and higher bandwidth than current networks. This will enable new applications such as virtual and augmented reality, as well as enable the growth of autonomous vehicles and smart cities. Data communication has also led to the growth of social media, which has transformed the way we communicate with one another. Social media platforms such as Facebook, Twitter, and Instagram have become an essential part of many people's lives, enabling them to connect with friends and family, share information, and engage with businesses and organizations[11], [12].

Overall, data communication has had a profound impact on society, enabling us to connect with one another and exchange information quickly and efficiently. As technology continues to evolve, we can expect to see even more innovations in data communication that will further transform the way we live and work. However, it is essential to be aware of the potential risks and challenges that come with data communication and take steps to mitigate them to ensure the security and reliability of the data being transmitted.

The seven layers of the OSI model are:

1. **Physical layer:** This layer is responsible for transmitting data over the physical communication channel. It is concerned with the physical characteristics of the communication channel, such as voltage, frequency, and bandwidth.
2. **Data link layer:** This layer is responsible for transmitting data over a link between two devices. It is concerned with error detection and correction, flow control, and access control.
3. **Network layer:** This layer is responsible for routing data between networks. It is concerned with addressing and forwarding data packets between devices on different networks.
4. **Transport layer:** This layer is responsible for the end-to-end delivery of data between devices. It is concerned with reliable data delivery, error detection and correction, flow control, and congestion control.
5. **Session layer:** This layer is responsible for establishing, maintaining, and terminating sessions between devices. It is concerned with session management, synchronization, and recovery.
6. **Presentation layer:** This layer is responsible for presenting data to the application layer in a format that can be understood by the application. It is concerned with data compression, encryption, and decryption.

7. **Application layer:** This layer is responsible for providing services to the user or application. It is concerned with the user interface, data storage and retrieval, and application-specific protocols.

Advancements in Data Communication

Data communication has evolved significantly over the years, driven by advances in technology and the increasing demand for faster and more efficient communication. Some of the significant advancements in data communication include:

1. **High-speed internet:** The advent of broadband internet has revolutionized data communication, enabling faster and more efficient data transfer.
2. **Wireless technology:** The development of wireless technologies such as Wi-Fi, Bluetooth, and cellular networks has enabled mobile communication and provided ubiquitous connectivity.
3. **Cloud Computing:**Cloud computing has enabled the storage and processing of data in the cloud, providing scalable and flexible computing resources to businesses and individuals.
4. **Internet of Things (IoT):** The IoT refers to the interconnectivity of devices and objects over the internet. The IoT has the potential to revolutionize data communication by enabling the collection and analysis of data from a wide range of devices and objects.

CONCLUSION

Data communication is an essential aspect of modern communication, enabling the transfer of digital data between devices and networks. It encompasses various components, including communication channels, protocols, and standards. The OSI model provides a framework for understanding how data is transmitted over a network. Advancements in technology have revolutionized data communication, enabling faster, more efficient, and ubiquitous connectivity. As technology continues to advance, data communication will continue to evolve, providing new opportunities and challenges for businesses and individuals alike.

REFERENCES

[1] J. Wang, M. Chen, J. Zhou, and P. Li, “Data communication mechanism for greenhouse environment monitoring and control: An agent-based IoT system,” *Inf. Process. Agric.*, 2020, doi: 10.1016/j.inpa.2019.11.002.

[2] J. Kim, S. S. Lee, J. Seo, and V. R. Kamat, “Modular data communication methods for a robotic excavator,” *Autom. Constr.*, 2018, doi: 10.1016/j.autcon.2018.02.007.

[3] B. J. Zikmund-Fisher, “Helping People Know Whether Measurements Have Good or Bad Implications: Increasing the Evaluability of Health and Science Data Communications,” *Policy Insights from Behav. Brain Sci.*, 2019, doi: 10.1177/2372732218813377.

[4] M. M. A. Eid, A. S. Seliem, A. N. Zaki Rashed, A. E. N. A. Mohammed, M. Y. Ali, and S. S. Abaza, “High sensitivity sapphire FBG temperature sensors for the signal processing of data communications technology,” *Indones. J. Electr. Eng. Comput. Sci.*, 2021, doi: 10.11591/ijeecs.v21.i3.pp1567-1574.

[5] C. Xiong, L. Van Weelden, and S. Franconeri, "The Curse of Knowledge in Visual Data Communication," *IEEE Trans. Vis. Comput. Graph.*, 2020, doi: 10.1109/TVCG.2019.2917689.

[6] C. Huang and Y. Huang, "Research and design of data communication subsystem of urban rail transit CBTC system," *Int. J. Syst. Assur. Eng. Manag.*, 2021, doi: 10.1007/s13198-021-01055-5.

[7] V. Moorthy, R. Venkataraman, and T. Rama Rao, "Security and privacy attacks during data communication in Software Defined Mobile Clouds," *Comput. Commun.*, 2020, doi: 10.1016/j.comcom.2020.02.030.

[8] S. Rajbhandari *et al.*, "A review of gallium nitride LEDs for multi-gigabit-per-second visible light data communications," *Semiconductor Science and Technology*. 2017. doi: 10.1088/1361-6641/32/2/023001.

[9] M. P. da Costa and F. C. Lima Leite, "Factors influencing research data communication on Zika virus: a grounded theory," *J. Doc.*, 2019, doi: 10.1108/JD-05-2018-0071.

[10] C. V. Poulton *et al.*, "Long-Range LiDAR and Free-Space Data Communication with High-Performance Optical Phased Arrays," *IEEE J. Sel. Top. Quantum Electron.*, 2019, doi: 10.1109/JSTQE.2019.2908555.

[11] C. Partridge, "Important concepts in data communications," *Comput. Commun. Rev.*, 2022, doi: 10.1145/3523230.3523237.

[12] S. L. Franconeri, L. M. Padilla, P. Shah, J. M. Zacks, and J. Hullman, "The Science of Visual Data Communication: What Works," *Psychol. Sci. Public Interes.*, 2021, doi: 10.1177/15291006211051956.

CHAPTER 2

INTERCONNECTING NETWORKS: A REVIEW OF TOPOLOGIES, PROTOCOLS, AND EMERGING TECHNOLOGIES FOR SCALABLE AND RELIABLE COMMUNICATION

Dr. Pooja Sagar, Assistant Professor,
Department of Computer Science, Sanskriti University, Mathura, Uttar Pradesh, India
Email id- pooja@sanskriti.edu.in

ABSTRACT:

The interconnection of networks refers to the process of connecting multiple computer networks together to create a larger, more comprehensive network. The interconnection of networks has become increasingly important as the number of devices and networks has grown, and it has enabled the creation of a global network that allows people and organizations to communicate and exchange information quickly and efficiently. The process of interconnecting networks involves the use of various techniques and technologies, including routers, switches, and protocols, and it requires careful planning and management to ensure that the networks can communicate effectively and securely.

KEYWORDS:

Computer Network, Interconnection Network, Technology, Routers.

INTRODUCTION

Interconnection of networks refers to the process of linking multiple networks so that they can communicate with each other. This is achieved through the use of protocols, hardware, and software that enable the transmission and reception of data across different networks.Interconnection of networks has been a crucial aspect of the growth and development of the internet. The internet is a vast network of interconnected networks that allows users to communicate and share information from any part of the world. The internet has revolutionized the way we work, communicate, and access information [1]–[3].

Interconnection of networks has also played a critical role in the growth and development of the telecommunications industry. Telecommunications is the transmission of information over long distances using electronic or optical signals. The telecommunications industry has experienced significant growth over the years, driven by advances in technology and the interconnection of networks. One of the key benefits of interconnection of networks is the ability to connect people and organizations across different locations. This has been particularly important for businesses that operate across different countries and continents.

The interconnection of networks has made it possible for businesses to communicate with their customers and partners, access information, and collaborate in real-time. Another benefit of interconnection of networks is the ability to share resources across different networks. This includes sharing of computing power, storage, and software applications. This has enabled organizations to optimize their resources and reduce costs [4]. Interconnection of networks has also enabled the creation of new services and applications that were not possible before. For example, the internet has enabled the creation of e-commerce platforms, social media platforms,

and online marketplaces. These services and applications have had a significant impact on how we live and work.In order to achieve interconnection of networks, several protocols and technologies have been developed. These include the Internet Protocol (IP), Transmission Control Protocol (TCP), User Datagram Protocol (UDP), Domain Name System (DNS), and Simple Network Management Protocol (SNMP). These protocols enable the transmission and reception of data across different networks.

In addition to protocols, hardware and software are also required to achieve interconnection of networks. This includes routers, switches, gateways, and firewalls. These devices are used to connect different networks and to control the flow of data between them. One of the key challenges of interconnection of networks is ensuring security and privacy. As networks become more interconnected, the risk of cyber-attacks and data breaches increases. This has led to the development of several security protocols and technologies, including Virtual Private Networks (VPNs), Secure Sockets Layer (SSL), and Transport Layer Security (TLS). Interconnection of networks has also led to the development of new business models and revenue streams. For example, many companies have started offering cloud-based services, where they provide computing power, storage, and software applications over the internet. This has enabled businesses to scale up their operations without having to invest in expensive hardware and software [5], [6].

Interconnection of networks has also played a critical role in the growth and development of the Internet of Things (IoT). The IoT is a network of interconnected devices that can communicate with each other and with other systems over the internet. The IoT has enabled the creation of new applications and services, such as smart homes, smart cities, and smart transportation systems. Interconnection of networks refers to the process of linking different computer networks together so that they can communicate and share resources. This can be done through various methods such as physical cabling, wireless connections, and software solutions. Interconnecting networks allows for improved communication, increased functionality, and enhanced collaboration between users and systems.

The concept of interconnecting networks is not a new one. In fact, it has been around since the early days of computing when people began to connect their computers together to share resources and data. However, as technology has advanced, so too has the need for interconnecting networks. Today, businesses, governments, and individuals rely on interconnected networks for everything from accessing the internet to sharing data with colleagues and clients around the world. There are many different types of networks that can be interconnected, including local area networks (LANs), wide area networks (WANs), and metropolitan area networks (MANs). Each of these networks has its own unique characteristics and requirements, but they can all be interconnected to create a more powerful and versatile network infrastructure. Interconnection can be achieved in several ways, including through physical connections such as cabling or wireless technologies, as well as through software solutions such as virtual private networks (VPNs) and cloud computing services. Let's take a closer look at each of these methods and the benefits they offer.

DISCUSSION

Physical Connections One of the most common methods of interconnecting networks is through physical connections, such as cabling or wireless technologies. This involves connecting two or more networks through physical means, such as running an Ethernet cable between two computers or setting up a wireless access point to connect to a Wi-Fi network.

Physical connections can be used to interconnect LANs, WANs, and MANs, and they offer several benefits. For example, they are generally more reliable than software solutions because they are less likely to be affected by issues such as network congestion or software bugs. Additionally, physical connections can offer faster data transfer rates than software solutions, which is important for organizations that need to transfer large amounts of data quickly[7], [8].Wireless technologies, such as Wi-Fi and Bluetooth, have become increasingly popular in recent years because they offer a convenient and flexible way to interconnect networks without the need for physical cables. Wireless connections can be used to interconnect devices within a LAN or to connect to a WAN or the internet. However, wireless connections are often less reliable and slower than physical connections, especially over longer distances or in areas with heavy network congestion.

In addition to physical connections, networks can also be interconnected through software solutions such as VPNs and cloud computing services. These solutions offer several benefits over physical connections, including greater flexibility and scalability, and they can often be more cost-effective. VPNs are a popular way to interconnect networks, particularly for remote workers or organizations with multiple offices. A VPN allows users to securely connect to a network over the internet, creating a virtual "tunnel" through which data can be transmitted. This provides a secure and private way to access resources on a network, and it can be particularly useful for organizations that need to share confidential information.

Cloud computing services, such as Amazon Web Services and Microsoft Azure, offer another way to interconnect networks. These services allow organizations to run applications and store data in the cloud, rather than on local servers or computers. This can be a cost-effective way to scale a network, as it eliminates the need for expensive hardware and infrastructure. Cloud computing services can also provide greater reliability and flexibility, as they are often backed by redundant systems and can be accessed from anywhere with an internet connection.

Interconnecting networks allows users to communicate and collaborate more effectively, interconnected networks can provide access to a wider range of resources and services, such as shared printers, files, and applications. This can improve productivity and efficiency by reducing the need for duplicate resources and enabling users to work more collaboratively. Interconnecting networks can provide greater flexibility in terms of where and how users can access resources. For example, a VPN can allow remote workers to securely connect to a network from anywhere in the world, while cloud computing services can provide access to applications and data from any device with an internet connection.

Interconnecting networks can be a cost-effective way to share resources and services, as it eliminates the need for duplicate hardware and infrastructure. Additionally, cloud computing services can provide a pay-as-you-go model that allows organizations to scale up or down as needed. Interconnecting networks can provide greater security by enabling organizations to enforce access controls and monitor network activity more closely. For example, a VPN can provide a secure way for remote workers to access sensitive data, while cloud computing services can provide advanced security features such as encryption and multi-factor authentication.

Interconnecting networks can be challenging if the networks are not compatible with each other. This can result in issues such as slow data transfer rates or dropped connections. Interconnecting networks can create security risks, particularly if sensitive data is being transmitted between the

networks. Organizations need to take steps to secure their networks and monitor network activity to ensure that unauthorized access is prevented.

Interconnecting networks can create management complexity, particularly if the networks are spread out across multiple locations. Organizations need to have the resources and expertise to manage and maintain their networks effectively. Interconnecting networks can result in performance issues, particularly if the networks are not optimized for the traffic that is being transmitted between them. Organizations need to ensure that their networks are properly configured and optimized to ensure maximum performance.

These days, it is quite uncommon to find a LAN, MAN, or LAN operating alone; they are all interconnected. An internetwork or internet is created when two or more networks are linked together. Consider, for instance, a business with two locations, one on the east coast one on the west coast, and the other. The freshly built east coast office has a star topology LAN, whereas the long-standing west coast office has a bus topology LAN. The company's president, who resides somewhere in the center, must exercise authority over the business.A switched WAN (run by a service provider like a telecom company) has been leased to link these three organizations (two LANs and the president's PC) as a backbone WAN. Yet three point-to-point WANs are needed to link the LANs to this switched WAN. These point-to-point WANs might be high-speed DSL lines provided by telephone companies or cable modern lines provided by cable TV providers.

Several facets of our everyday life have been changed by the Internet. Both our daily activities and our leisure time have been impacted by it. How often have you lately utilized the Internet? You may have used the Internet to send an e-mail to a business contact, pay a utility bill, read a newspaper from a different city, or search up a local movie schedule. Or maybe you looked up a medical subject, made a hotel reservation, spoke to another Trekked, or did some automobile comparison shopping. We now have access to a plethora of information that has been arranged for our benefit thanks to the communication system known as the Internet [9].

The Internet is a well-organized and structured system. A quick overview of the Internet's history comes first. The current state of the Internet is described after that. A network is a collection of linked communication devices, such printers and computers. Two or more networks that can connect with one another are considered to be part of the internet notice the lowercase the Internet, which starts with an initial I, is the most well-known internet and is made up of more than a million linked networks. The Internet is used by private persons as well as many organizations throughout the world, including government organizations, institutions of higher learning, businesses, and libraries. There are millions of users. Yet this remarkable communication mechanism didn't exist until 1969.Mainframe computers were independent equipment in research groups in the middle of the 1960s. The computers couldn't talk to each other since they were made by separate companies. In order for the researchers they financed to communicate their discoveries and cut down on expenses and duplication of effort, the Department of Defense's Advanced Research Projects Agency (ARPA) was interested in finding a mechanism to link computers.

A tiny network of interconnected computers called ARPANET was first proposed by ARPA in 1967 at a conference of the Association for Computing Machinery (ACM). The plan was for each host computer which did not have to be made by the same company to be connected to an interface message processor (IMP). In sum, the IMPs would be linked to one another. Each IMP

has to be able to interact with both its associated host and other IMPs. The ARPANET had been created by 1969. A network was created by connecting four nodes located at the University of Utah, Stanford Research Institute, University of California at Santa Barbara, and University of California at Los Angeles through IMPs. The Network Control Protocol (NCP) was a piece of software that allowed communication between the hosts.

Vint Cerf and Bob Kahn, who were both members of the core ARPANET group, worked together on the Internetting Project in 1972. The methods to ensure end-to-end packet delivery were specified in the seminal article by Cerf and Kahn published in 1973. Encapsulation, the datagram, and the purposes of a gateway were all discussed in this Transmission Control Protocol (TCP) study. Soon after, authorities decided to divide TCP into the Internetworking Protocol (IPP) and Transmission Control Protocol (TCP) (lP). TCP would be in charge of higher-level tasks like segmentation, reassembly, and error detection while IP would handle datagram routing. As TCPIIP, the internetworking protocol is currently known.

During the 1960s, the Internet has developed significantly. Today's Internet does not simply follow a hierarchical structure. It is composed of several wide- and local-area networks connected by switching stations and connecting hardware. Given that the Internet is always evolving new networks are added, old networks get new addresses, and networks belonging to out-of-business organisations are removed it is challenging to portray it accurately. The majority of consumers nowadays who desire Internet access utilize internet service providers' services (lSPs). There are service providers from all over the world.

The backbone networks used by the national Internet service providers were built and are still maintained by specialist businesses. North America is home to a large number of national ISPs, among of the most well-known of which are SprintLink, PSINet, UUNet Technologies, AGIS, and internet Mel. These backbone networks are linked by intricate switching facilities called network access points, which are often managed by a third party, to enable communication between the end customers (NAPs). Peering points are privately owned switching facilities that link certain national ISP networks. Often, they have a high data rate (up to 600 Mbps). Smaller internet service providers, sometimes known as regional ISPs, are interconnected with one or more national ISPs. With a lower data rate, they are in the third rung of the hierarchy.

End customers get direct service from local Internet service providers. Local ISPs may be linked directly to national ISPs, regional ISPs, or both. The majority of end customers are linked to regional ISPs. It should be noted that a local ISP in this context might be a business that just offers Internet services, a firm with a network that serves its own workers, or a nonprofit institution like a college or university that manages its own network. Every one of these neighborhood ISPs is able to connect to a local or national service provider.

Communication takes place in computer networks between components of various systems. Everything that can transmit or receive information is considered an entity. Nevertheless, two entities cannot just exchange bit streams and expect to understand one another. The entities must agree on a protocol for communication to take place. Data transmission is governed by a set of rules known as a protocol. What is sent, how it is communicated, and when it is communicated are all specified by a protocol. Syntax, semantics, and timing are a protocol's three main components.

Grammar. The word syntax describes the organisation or arrangement of the data, i.e., the sequence in which it is presented. For instance, a straightforward protocol may assume that the first 8 bits of data are the sender's address, the next 8 bits are the receiver's address, and the remaining data is the message itself the semantics. The meaning of each bit's segment is referred to as its semantics. What should be done based on an interpretation of a certain pattern and how should that interpretation be applied? Does an address, for instance, specify the route to be taken or the intended recipient of the message?

Momentum. Timing describes two aspects: when data should be sent and how quickly it can be sent. For instance, a transmission would overwhelm the receiver if the sender generates data at 100 Mbps while the receiver can only handle data at 1 Mbps [10]. Standards are crucial for establishing and preserving an open and competitive market for equipment makers as well as for ensuring the interoperability of data and telecommunications technologies and procedures on a national and worldwide level. Standards provide manufacturers, suppliers, government organizations, and other service provider's standards to assure the level of interconnectivity required in today's market and in international communications

In actuality standards are those that have been accepted as norms despite not having received formal approval from a governing organization. Manufacturers that want to describe the functioning of a new product or technology often create de facto standards in the beginning. Data telecommunications in North America generally depend on those produced by the following organizations, despite the fact that several are devoted to the production of standards:

The ISO is a global organization whose members are mostly recruited from the committees charged with developing international standards for different countries. The ISO actively promotes collaboration in the fields of science, technology, and business. The Telecommunication Standards Section of the International Telecommunication Union (ITU-T). While several nations had established national telecommunications standards by the early 1970s, there was still minimal cross-border interoperability. The International Telecommunication Union (ITU) of the United Nations reacted by creating a group called the Consultative Committee for International Telegraphy and Telephony (CCITT). This group was responsible for doing research and developing standards for data and phone networks in particular, as well as for telecommunications in general. This committee's name was changed to the International Telecommunication Union Telecommunication Standards.

Despite its name, the American National Standards Institute is a totally independent nonprofit organisation that is not connected to the federal government of the United States. The wellbeing of the United States and its residents, however, takes precedence over all ANSI operations. The biggest professional engineering society in the world is the Institute of Electrical and Electronics Engineers. Its goal is to enhance theory, innovation, and product quality in the domains of electrical engineering, electronics, and radio as well as in all other engineering branches. It is an international endeavour. The IEEE has as one of its objectives to supervise the creation and implementation of global standards for communications and computers.

The Electronic Industries Association, a nonprofit with ANSI alignment, promotes electronics industry issues. In addition to developing standards, it also engages in lobbying and public awareness-raising initiatives. The EIA defined physical connection interfaces and electrical signaling requirements for data exchange, making substantial contributions to the area of information technology.

The advancement of telecommunications technology is occurring more quickly than the capacity of standards groups to approve standards. Standards committees are formal organizations that move slowly by design. Several special-interest groups have created forums made up of representatives from interested firms in order to fulfil the need for working models and agreements and to aid the standardization process. The forums test, assess, and standardize new technologies in collaboration with academic institutions and users. The forums are able to hasten adoption and deployment of certain technologies in the telecommunications industry by focusing their efforts on that technology.

The forums inform the standards organizations of their findings. Governmental organisations, such the Federal Communications Commission (FCC) in the United States, have the authority to regulate all forms of communication technology[11]. These organisations' mandate is to safeguard the public interest via the regulation of wire or cable communications, radio, and television. When it comes to communications, the FCC has control over both domestic and foreign trade.

A properly validated specification that is followed by individuals who operate with the Internet is known as an Internet standard. It is a formal rule that must be complied with. A specification must follow a rigorous process before becoming an Internet standard. A specification first appears online as a draught. An Internet draught is a work-in-progress with a six-month lifespan and no formal status. A draught may be released as a Request for Comments upon advice from the Internet authorities (RFC). Each RFC is revised, given a number, and made accessible to all parties involved. RFCs are classified and go through maturity stages based on the degree of requirements.

CONCLUSION

Interconnecting networks is a critical part of modern computing, enabling users and organizations to communicate and collaborate more effectively, access a wider range of resources and services, and reduce costs. Physical connections and software solutions such as VPNs and cloud computing services offer different benefits and challenges, and organizations need to carefully consider their needs and requirements when choosing the best approach. The benefits of interconnecting networks far outweigh the challenges, and organizations that take the time to plan and implement their networks effectively will be well-positioned to succeed in today's interconnected world.

REFERENCES

[1] A. Erickson, I. A. Stewart, J. Navaridas, and A. E. Kiasari, “The stellar transformation: From interconnection networks to datacenter networks,” *Comput. Networks*, 2017, doi: 10.1016/j.comnet.2016.12.001.

[2] O. A. Amodu, M. Othman, N. A. M. Yunus, and Z. M. Hanapi, “A primer on design aspects and recent advances in shuffle exchange multistage interconnection networks,” *Symmetry (Basel).*, 2021, doi: 10.3390/sym13030378.

[3] S. M. Nabavinejad, M. Baharloo, K. C. Chen, M. Palesi, T. Kogel, and M. Ebrahimi, “An Overview of Efficient Interconnection Networks for Deep Neural Network Accelerators,” *IEEE J. Emerg. Sel. Top. Circuits Syst.*, 2020, doi: 10.1109/JETCAS.2020.3022920.

[4] J. D. Owens, W. J. Dally, R. Ho, D. N. Jayashima, S. W. Keckler, and L. S. Peh, "Research challenges for on-chip interconnection networks," *IEEE Micro*, 2007, doi: 10.1109/MM.2007.4378787.

[5] A. Aljawawdeh, E. Emriziq, and S. Manaseer, "Triangle hyper Hexa-cell interconnection network a novel interconnection network," *Int. J. Adv. Comput. Sci. Appl.*, 2019, doi: 10.14569/IJACSA.2019.0100378.

[6] F. Al Faisal, M. M. Hafizur Rahman, and Y. Inoguchi, "HFBN: An Energy Efficient High Performance Hierarchical Interconnection Network for Exascale Supercomputer," *IEEE Access*, 2022, doi: 10.1109/ACCESS.2021.3138828.

[7] N. A. Md Yunus, M. Othman, Z. Mohd Hanapi, and K. Y. Lun, "Reliability Review of Interconnection Networks," *IETE Technical Review (Institution of Electronics and Telecommunication Engineers, India)*. 2016. doi: 10.1080/02564602.2015.1130595.

[8] P. K. Tripathy, R. K. Dash, and C. R. Tripathy, "A dynamic programming approach for layout optimization of interconnection networks," *Eng. Sci. Technol. an Int. J.*, 2015, doi: 10.1016/j.jestch.2015.01.003.

[9] E. Cheng, K. Qiu, and Z. Shen, "Diagnosability of interconnection networks: past, present and future," *Int. J. Parallel, Emergent Distrib. Syst.*, 2020, doi: 10.1080/17445760.2019.1655742.

[10] R. Trobec, R. Vasiljević, M. Tomašević, V. Milutinović, R. Beivide, and M. Valero, "Interconnection networks in petascale computer systems: A survey," *ACM Comput. Surv.*, 2016, doi: 10.1145/2983387.

[11] M. N. M. Ali *et al.*, "SCCN: A Time-Effective Hierarchical Interconnection Network for Network-On-Chip," *Mob. Networks Appl.*, 2019, doi: 10.1007/s11036-019-01262-2.

CHAPTER 3

ANALYSIS AND COMPARISON OF NETWORK MODELS: A COMPREHENSIVE STUDY ON GRAPH THEORY, MACHINE LEARNING, AND STATISTICAL APPROACHES FOR NETWORK ANALYSIS

Dr. Lokesh Kumar, Assistant Professor,
Department of Computer Science, Sanskriti University, Mathura, Uttar Pradesh, India,
Email id- lokesh@sanskriti.edu.in

ABSTRACT:

Network models are mathematical representations of complex systems that are composed of interconnected nodes or entities. These models are used to analyze and understand the behavior of various systems, such as social networks, transportation networks, and electrical power grids, among others. One of the most important applications of network models is in understanding the spread of information, diseases, and other phenomena through the network. By analyzing the structure and properties of a network, researchers can identify key nodes or entities that are most influential in the spread of information or disease, and develop strategies to prevent or control its spread.

KEYWORDS:

Complex System, Network Model, Key Nodes, Power Grids, Systems.

INTRODUCTION

A network model is a conceptual representation of a network, which is a collection of interconnected nodes or points that are linked together by edges or lines. These models are used to study and analyze the behavior of different types of networks, including computer networks, social networks, transportation networks, and many others. There are many different types of network models, each with its own set of assumptions, rules, and parameters. Some of the most commonly used models include the random graph model, small-world model, scale-free model, and network formation model [1]–[3] .

The random graph model is one of the simplest network models, and it assumes that edges are randomly generated between nodes with a fixed probability. In this model, each node is equally likely to be connected to any other node, and the resulting network has a uniform distribution of edge density. The small-world model, on the other hand, assumes that most nodes are not directly connected, but are instead linked together through a small number of highly connected nodes, or "hubs". This model was first proposed by social psychologist Stanley Milgram in the 1960s, and it has since been applied to a wide range of real-world networks.

The scale-free model is another popular network model, and it assumes that most nodes have only a few connections, but a small number of nodes have a large number of connections [4]. This type of network is said to be "scale-free" because the distribution of node degrees (i.e. the number of connections each node has) follows a power law, rather than a normal distribution. Finally, the network formation model is a more general framework that can be used to study how networks are formed and evolve over time. This model is based on the idea that nodes form connections based on some sort of underlying "preference" or "attachment" mechanism, which

can depend on factors such as geographical proximity, shared interests, or prior connections. One of the key applications of network models is in the analysis of social networks. Social networks are collections of individuals or organizations that are linked together by various types of social relationships, such as friendship, professional relationships, and family ties. By modeling these networks, researchers can gain insights into how information flows through the network, how influence is spread, and how communities and subgroups form [5], [6].

Another important application of network models is in the study of transportation networks. These networks include highways, railways, air routes, and other forms of transportation infrastructure. By modeling these networks, researchers can gain insights into traffic flow patterns, optimal routing strategies, and the impact of different types of disruptions on the network as a whole. In addition to social and transportation networks, network models are also used to study a wide range of other complex systems, including ecological networks, financial networks, and biological networks. In each of these cases, the network model provides a useful framework for understanding the behavior of the system as a whole, as well as the interactions between individual components.

Despite their usefulness, network models also have some limitations. For example, they often rely on simplifying assumptions that may not accurately reflect the real-world system being studied. In addition, the complexity of the model can make it difficult to interpret the results or identify the most important factors driving network behavior[7], [8]. To address these limitations, researchers are continually developing new and more sophisticated network models, as well as new methods for analyzing and interpreting network data. By combining these models with real-world data, researchers are able to gain increasingly detailed insights into the structure and behavior of complex systems, and to develop new strategies for optimizing their performance and resilience.

A network is a collection of hardware and software that transfers data between two or more locations. The physical tools used to transmit signals across the network are referred to as hardware. The programme is made up of sets of instructions that maybe the network services that we demand. A network model is a mathematical model that is used to represent complex systems or relationships. Network models can be applied to a wide range of fields, including computer science, social science, biology, and many others. In this article, we will discuss the basics of network models, their types, and their applications.

DISCUSSION

Introduction to Network Models a network model is a mathematical representation of a system or a group of objects. In a network model, the objects are represented by nodes or vertices, and the relationships between them are represented by edges or links. The edges can have different properties, such as weights or direction, depending on the application. Network models are used to study the structure and behavior of complex systems, such as social networks, transportation networks, biological systems, and computer networks. They help us to understand the patterns of interactions between the objects in the system, identify important nodes and links, and predict the behavior of the system under different conditions.Undirected graphs are network models in which the edges have no direction. In an undirected graph, the relationship between two nodes is symmetrical, and the edge can be traversed in either direction. For example, a social network can be represented as an undirected graph, where the nodes are the users, and the edges represent their friendships. Directed graphs are network models in which the edges have a direction. In a

directed graph, the relationship between two nodes is asymmetric, and the edge can only be traversed in one direction. For example, a transportation network can be represented as a directed graph, where the nodes are the cities, and the edges represent the one-way roads.

Weighted graphs are network models in which the edges have a weight or a value. In a weighted graph, the weight of an edge can represent a variety of properties, such as the distance between two nodes, the strength of a relationship, or the cost of a transaction. For example, a financial network can be represented as a weighted graph, where the nodes are the accounts, and the edges represent the transactions, with the weight representing the amount of money transferred. Bipartite graphs are network models in which the nodes can be divided into two disjoint sets. In a bipartite graph, the edges only connect nodes from different sets, and there are no edges between nodes in the same set. For example, a movie recommendation system can be represented as a bipartite graph, where one set of nodes represents the users, and the other set represents the movies, and the edges represent the ratings given by the users.

Hyper graphs are network models in which the edges can connect more than two nodes. In a hyper graph, the edges can be represented as sets of nodes, and the nodes can be connected to multiple edges. For example, a web page network can be represented as a hyper graph, where the nodes are the web pages, and the edges represent the hyperlinks, which can connect more than two web pages. Social networks can be represented as network models, where the nodes are the individuals, and the edges represent their relationships. By analyzing social network models, we can study the patterns of interactions between individuals, identify the influential individuals, and predict the spread of information or diseases.

Transportation networks can be represented as network models, where the nodes are the cities or the transportation hubs, and the edges represent the roads, railways, or airlines. By analyzing transportation network models, we can study the efficiency job of networking may be compared to the challenge of using a computer to solve a mathematical problem. Computer hardware handles the primary function of using a computer to solve the issue. If just hardware is involved, this is a fairly laborious job.

Every memory region would need a switch in order to store and alter data. If software is available, the work is significantly simpler. At the highest level, a programmed may control how problems are solved; the specifics of how this is carried out by the hardware itself can be left to the layers of software that the higher levels call. This may be compared to a service offered by a computer network. For instance, sending an email from one location in the globe to another may be divided into multiple jobs, each of which is handled by a different piece of software. Each software programmer makes use of the capabilities of other software programmed. A signal, or group of signals, are sent from the source computer to the destination computer at the lowest layer.

We provide a broad overview of a network's levels in this chapter and go through each layer's purposes. Further chapters provide in-depth explanations of various strata. Let's start by outlining the events that occur at the sender site in chronological sequence. A deeper layer. The letter is written, placed in an envelope, with the sender's and recipient's addresses written on it, and then the letter is placed in a mailbox. In the middle. A letter carrier picks up the mail and delivers it to the post office. The receiver will then get the letter. The mail may really pass via a central office on route to the recipient's neighborhood post office. It may also be sent by truck, rail, aircraft, boat, or a combination of these modes of transportation.

Bottom layer at the receiver site. The mail is delivered by the carrier to the post office. Our research shows that the sender site has three distinct activities, while the recipient site has three more activities. The carrier is responsible for moving the letter between the sender and the recipient. The need of doing the duties in the hierarchy's sequence is something that is not immediately clear. The letter must be written at the sender's location, placed in the mailbox, picked up by the letter carrier, and delivered to the post office. The letter must be delivered to the recipient's location and placed in their mailbox before being picked up and read by them.

At the transmitting site, each layer utilizes the services of the layer below it. The intermediary layer's services are used by the sender at the upper tier. The lowest layer provides its services to the intermediate layer. The carrier's services are used by the bottom layer. Until 1990, the Open Systems Interconnection (OSI) model was the layered paradigm that dominated the literature on data communications and networking. The OSI model was thought to be the gold standard for data transmission, however this did not materialize. Due to significant usage and testing on the Internet, the TCPIIP protocol suite replaced the OSI model as the preeminent commercial architecture.

The International Standards Organization (ISO), a multinational organization founded in 1947, works to promote global consensus on international standards. The Open Systems Interconnection model is an ISO standard that addresses every facet of network communications. In the late 1970s, it was initially made available. A collection of protocols known as a "open system" enables any two separate systems, regardless of their underlying architecture, to interact with one another. The OSI model demonstrates ways to improve communication across various systems without having to alter the hardware or software's basic logic. The OSI model is not a protocol; rather, it provides a framework for comprehending and creating a flexible, reliable, and interoperable network architecture [9].

Many different kinds of computer systems may communicate with one another thanks to the OSI model, which is a layered foundation for network system architecture. It is made up of seven distinct but interconnected layers, each of which specifies a step in the transfer of information across a network. The OSI model's foundational concepts provide a strong foundation for investigating data communications. The model's creators reduced the data transmission mechanism to its most basic components while creating it. The networking functions that had similar needs were gathered into distinct groupings, which eventually formed the layers. A family of functions unique from those of the other levels is defined by each layer. In this way, the designers defined and localized functions to produce a complete and adaptable architecture. Most crucially, the OSI paradigm enables total interoperability between systems that would not otherwise be compatible.

Each layer inside a single machine uses the resources of the layer directly underneath it. For instance, layer 3 consumes the services offered by layer 2 and offers services to layer 4. Layer X on one computer talks to Layer X on another machine across machines. Protocols are an established set of guidelines and practises that regulate this communication. Peer-to-peer processes are those on each system that interact at a certain layer. In order to communicate between machines, a peer-to-peer mechanism employing protocols specific to a certain layer is used.Physical layer communication is straightforward: Device A transmits a stream of bits to Device B. (through intermediate nodes). But, in the upper levels, communication must go from device A to device B and back again across the layers. Physical communication that travels up

via the layers. In the transmitting device, each layer transfers the whole package to the layer immediately below it after adding its own information to the message it gets from the layer immediately above it. The whole package is transformed at layer I into a format that can be sent to the receiving device. The message is unwrapped layer by layer at the receiving computer, with each operation taking in and discarding the data intended for it. For instance, layer 2 transfers the remaining data to layer 3 after removing the data intended for it. The remaining data is then sent to layer 4 after layer 3 has removed the information intended for it.

An interface between each pair of adjacent levels enables the transmission of data and network information down through the layers of the sending device and back up via the layers of the receiving device. The information and services that a layer must provide to the layer above it are defined by each interface. A network's modularity is provided via well-defined interfaces and layer functionalities. A layer's exact implementation of its functions may be changed or replaced without necessitating adjustments to the layers around it as long as it continues to offer the required services to the layer above it.

Three subgroups of the seven tiers may be conceptualized. The physical components of transporting data from one device to another, such as electrical specifications, physical connections, physical addressing, and transport timeliness and dependability, are dealt with by Layers I, 2, and 3 physical, data link, and network which constitute the network support layers. The user support layers 5, 6, and 7 are session, presentation, and application, respectively. They enable interoperability across unrelated software systems. The transport layer, which connects the two subgroups, makes sure that the information delivered by the lower levels is in a format that the top layers can understand.

Except for the physical layer, which is largely hardware, the top OSI layers are nearly always implemented in software; the lower levels are a mix of hardware and software. The OSI layers overall, shows D7 refers to the layer 7 data unit, D6 to the layer 6 data unit, and so on. The procedure proceeds layer by layer in decreasing, sequential sequence, beginning at layer 7 (the application layer). A header or maybe a trailer might be appended to the data unit at each tier. The trailer is often only included at layer 2. The prepared data unit is converted into an electromagnetic signal and sent through a physical connection as soon as it passes through the physical layer (layer 1).

As the signal gets there, it enters layer 1 and is converted back to digital form. After then, the data units ascend once again via the OSI layers. The headers and trailers that were connected to each data block at the associated sending layer are removed when the block moves up a layer, and the layer-specific operations are then carried out. As the communication reaches layer 7, it is once again accessible to the receiver in an application-appropriate form.

Encapsulation is another facet of data transmission in the OSI model. A level 7 packet (header and data) is included in a level 6 packet. A packet at level 5 encapsulates the whole packet at level 6, and so on. In other words, the level N–1 data section of a packet contains the whole level N packet, including data, header, and perhaps trailer. Level N–1 is unaware of which portion of an enclosed packet is data and which portion is the header or trailer; this phenomenon is known as encapsulation. Layers in the OSI model the whole packet originating from level N is regarded as one integral item for level N – 1. The roles of each layer in the OSI model are briefly described in this section.

The activities necessary to transmit a bit stream via a physical media are coordinated by the physical layer. It deals with the transmission medium's interface's mechanical and electrical requirements. Moreover, it specifies the practices and duties that hardware and interfaces must carry out for transmission to occur. The physical layer's relationship to the transmission medium and the data connection layer. The physical properties of the medium and interfaces. The interface properties between the devices and the transmission media are determined by the physical layer. Moreover, it specifies the kind of transmission media.

Bit representation. The data in the physical layer is just a stream of bits (a series of Os or 1s) without any meaning. Bits must be 34 in order to be sent encoded into signals, whether they be electrical or visual. The kind of encoding is determined by the physical layer (how Os and Is are changed to signals) data speed The physical layer also determines the transmission rate, or the number of bits transferred per second. In other words, the length of a bit, or how long it lasts, is defined by the physical layer. Bit synchronization In addition to using the same bit rate, the transmitter and receiver both need to be in sync at the bit level. In other words, the clocks of the transmitter and the receiver must be in sync. Line arrangement. The physical layer deals with how devices are connected to the media. A dedicated connection connects two devices in a point-to-point manner. Many devices share a connection in a multipoint arrangement.

Topology of matter. The physical topology specifies how elements of a network are linked together. Devices may be linked together using a bus topology every device is on a common connection, a ring topology each device is connected to the next, creating a ring, a mesh topology each device is connected to every other device), or a hybrid topology this is a mix of two or more topologies. Mode of transmission. Simplex, half-duplex, or full-duplex communication between two devices are all defined by the physical layer. Just one device can transmit in simplex mode; the other can only receive. Simplex is a one-way communication method. Two devices may transmit and receive in half-duplex mode, but not simultaneously. A full-duplex mode, often known as duplex mode, allows two devices to transmit and receive data simultaneously.

The physical layer, which is a crude transmission facility, is transformed into a dependable connection by the data link layer. It gives the network layer, the layer above, the impression that the physical layer is error-free. The connection between the data link layer and the network and physical layers. The transmission of frames from one hop (node) to the next is handled by the data link layer. The following are some of the additional duties of the data connection layer: The data link layer adds a header to the frame to specify the sender and/or recipient of the frame if frames need to be distributed across several computers on the network. The receiver address is the address of the device that links the sender's network to the system for which the frame is intended.

The data connection layer applies a flow control mechanism to prevent overloading the receiver if the rate at which data are created in the sender is slower than the rate at which data are consumed by the receiver.By introducing systems to identify and retransmit broken or missing frames, the data link layer increases dependability of the physical layer. Moreover, it employs a system to detect duplicate frames. Typically, a trailer is inserted at the end of the frame to accomplish error control.

Data link layer protocols are required when two or more devices are connected to the same connection in order to identify which device is in charge of the link at any given moment.The

graphic illustrates how two nearby nodes communicate with one another at the data connection layer. Three partial deliveries are done in order to transmit data from A to F. Initially, a frame is sent from data link layer A to data link layer B. (a router). Second, the data link layer at B delivers a fresh frame to the data link layer at E. A fresh frame is then sent to the data link layer at F via the data link layer at E. Keep in mind that the header values of the frames that are sent across the three nodes varies. B is the destination address and A is the source address for the frame travelling from A to B. E is the destination address and B is the source address in the frame going from B to E. F is the destination address and E is the source address for the frame travelling from E to F. If error checking includes the frame header, the values of the trailers may also change.

A packet must be delivered from source to destination via the network layer, maybe through many networks (links). The network layer makes sure that every packet travels from its place of origin to its ultimate destination, whereas the data link layer manages packet delivery between two systems connected by the same network (links). A network layer is often not required if two systems are linked to the same connection. Yet, source-to-destination delivery is often required by the network layer if the two systems are connected to distinct networks (links) by connecting devices between the networks (links). The connection between the network layer and the data link and transport layers.The data connection layer's physical addressing solution addresses the addressing issue locally. Another addressing scheme is required to assist differentiate the source and destination systems whenever a packet crosses the network border. The network layer adds a header, which among other things contains the logical addresses of the sender and recipient, to the packet that comes from the top layer. Later on in this chapter, we talk about logical addresses.

The connecting devices (known as routers) are used to join separate networks or connections to form networks of networks or massive networks or switches route or switch the packets to their ultimate destination.As the image demonstrates, now we require a source-to-destination delivery. The network layer a transfers the packet to the network layer at B. Based on the packet's eventual destination (F), router B decides what to do when it receives the packet. Later chapters will show how router B utilizes its routing database to determine that router E is the next hop. As a result, the packet is sent to the network layer at E by the network layer at B. The packet is sent to the network layer at F by the network layer at E in tum.

The full message must be sent from one process to another through the transport layer. An application programmed executing on a host is known as a process. Although the network layer manages source-to-destination packet delivery, it is blind to the relationships between the packets. Whether or whether each component is a part of a distinct message, it processes them all separately. The transport layer, on the other hand, is in charge of error control and flow control from the source to the destination level, making sure the whole message arrives intact and in the proper sequence.

Addressing at service points. Several applications are often running at once on computers. Because of this, source-to-destination delivery refers to the transfer of data from one computer to another as well as from one specific process (running programmed) to another specific process (running programed) on another computer. Therefore, a type of address known as a service-point address must be included in the transport layer header (or port address). The transport layer

delivers the entire message to the right process on that computer after the network layer routes each packet to the appropriate computer [10].

A message is broken up into segments that can be transmitted, and each segment has a unique sequence number. These numbers allow the transport layer to identify and replace packets that were lost during transmission and to correctly reassemble the message once it reaches its destination.Either a connectionless or connection-oriented transport layer is possible. Each segment is delivered to the destination machine's transport layer by a connectionless transport layer, which treats each one as a separate packet. Before sending the packets, a connection-oriented transport layer establishes a connection with the transport layer at the destination machine. The connection is cut off once all the data have been transferred. Flow control is handled by the transport layer, just like the data link layer. At this layer, flow control is handled end to end as opposed to across a single link.Like the data connection layer, the transport layer is responsible for error control. However, instead of across a single link, error control at this layer is carried out process-to-process. The sending transport layer ensures that there are no errors (damage, loss, or other issues) when the entire message reaches the receiving transport layer.

CONCLUSION

Network models are an essential tool for studying and understanding the behavior of complex systems. By providing a conceptual framework for representing the interactions between individual components, these models allow researchers to gain insights into the structure and function of a wide range of networks, including social networks, transportation networks, and many others [11]. While network models have some limitations, including simplifying assumptions and complex interpretations, ongoing research is continually developing new and more sophisticated models to better reflect the real-world systems being studied. This research is leading to new insights into how networks evolve over time, how they respond to disruptions, and how they can be optimized to perform more effectively.

REFERENCES

[1] J. M. B. Haslbeck, “Estimating group differences in network models using moderation analysis,” *Behav. Res. Methods*, 2022, doi: 10.3758/s13428-021-01637-y.

[2] J. M. B. Haslbeck and L. J. Waldorp, “How well do network models predict observations? On the importance of predictability in network models,” *Behav. Res. Methods*, 2018, doi: 10.3758/s13428-017-0910-x.

[3] J. M. B. Haslbeck, D. Borsboom, and L. J. Waldorp, “Moderated Network Models,” *Multivariate Behav. Res.*, 2021, doi: 10.1080/00273171.2019.1677207.

[4] M. Marsman *et al.*, “An Introduction to Network Psychometrics: Relating Ising Network Models to Item Response Theory Models,” *Multivariate Behav. Res.*, 2018, doi: 10.1080/00273171.2017.1379379.

[5] J. C. Baez, J. Foley, J. Moeller, and B. S. Pollard, “Network models,” *Theory Appl. Categ.*, 2020, doi: 10.4324/9781003179030-2.

[6] Z. Bi and C. Zhou, “Understanding the computation of time using neural network models,” *Proc. Natl. Acad. Sci. U. S. A.*, 2020, doi: 10.1073/pnas.1921609117.

[7] L. Xue *et al.*, "A data-driven network model for the emerging COVID-19 epidemics in Wuhan, Toronto and Italy," *Math. Biosci.*, 2020, doi: 10.1016/j.mbs.2020.108391.

[8] N. Kriegeskorte and T. Golan, "Neural network models and deep learning," *Current Biology*. 2019. doi: 10.1016/j.cub.2019.02.034.

[9] R. van Bork, M. Rhemtulla, L. J. Waldorp, J. Kruis, S. Rezvanifar, and D. Borsboom, "Latent Variable Models and Networks: Statistical Equivalence and Testability," *Multivariate Behav. Res.*, 2021, doi: 10.1080/00273171.2019.1672515.

[10] X. Zhang *et al.*, "Generative network models of altered structural brain connectivity in schizophrenia," *Neuroimage*, 2021, doi: 10.1016/j.neuroimage.2020.117510.

[11] A. M. Isvoranu, S. Epskamp, and M. W. L. Cheung, "Network Models of Posttraumatic Stress Disorder: A Meta-Analysis," *J. Abnorm. Psychol.*, 2021, doi: 10.1037/abn0000704.

CHAPTER 4

TCP/IP PROTOCOL SUITE: AN OVERVIEW AND ANALYSIS OF THE MOST WIDELY USED INTERNET PROTOCOL STACK IN THE WORLD

Dr. Himanshu Singh, Assistant Professor,
Department of Computer Science, Sanskriti University, Mathura, Uttar Pradesh, India,
Email id- himanshu.singh@sanskriti.edu.in

ABSTRACT:

The TCP/IP protocol suite is a set of communication protocols that govern the way data is transmitted over the internet. It consists of two main protocols: the Transmission Control Protocol (TCP) and the Internet Protocol (IP). IP is responsible for routing data between different networks, while TCP is responsible for ensuring the reliable delivery of data between hosts on a network. Other important protocols in the suite include the User Datagram Protocol (UDP) for lightweight communication, the Internet Control Message Protocol (ICMP) for diagnostic and error reporting, and the Address Resolution Protocol (ARP) for mapping network addresses to physical addresses.

KEYWORDS:

Address Resolution Protocol (ARP), Internet Protocol (IP), Transmission Control Protocol (TCP), User Datagram Protocol (UDP), Internet Control Message Protocol (ICMP).

INTRODUCTION

The TCP/IP Protocol Suite, also known as the Internet Protocol Suite, is a set of communication protocols used for communicating over the Internet and other computer networks. The name TCP/IP comes from two of the most important protocols in the suite: the Transmission Control Protocol (TCP) and the Internet Protocol (IP). TCP/IP was developed in the 1970s by the Department of Defense's Advanced Research Projects Agency (ARPA) as a means of connecting disparate computer networks together [1]–[3] .

TCP/IP is a layered protocol suite, meaning that it is organized into layers, each of which performs a specific function. The layers in TCP/IP are often referred to as the Internet protocol stack, and they are:

1. Application layer
2. Transport layer
3. Internet layer
4. Link layer

The application layer is the layer closest to the user and includes protocols such as HTTP, FTP, SMTP, and DNS. The transport layer is responsible for managing end-to-end connections and data transfer, and includes TCP and UDP. The internet layer provides routing and addressing functions and includes the IP protocol. The link layer is responsible for the physical transmission of data and includes protocols such as Ethernet and Wi-Fi[4] .

TCP/IP is the foundation of the modern Internet and is used for communication between all types of devices, including computers, smartphones, and IoT devices. While it was originally developed for use in military and academic settings, TCP/IP has become the de facto standard for network communication and is used by virtually every organization that uses the Internet.

TCP/IP is a connection-oriented protocol suite, which means that it establishes a connection between two devices before data can be exchanged. TCP provides reliable, error-checked delivery of data, while UDP provides a simpler, faster, but less reliable delivery mechanism. The IP protocol is responsible for routing packets between networks and ensuring that they are delivered to the correct destination. The TCP/IP protocol suite is designed to be open and extensible, which has enabled the development of a wide range of new protocols and applications that run on top of the existing TCP/IP protocols. For example, the Domain Name System (DNS) is an application that uses the TCP/IP suite to translate domain names into IP addresses, while the Simple Mail Transfer Protocol (SMTP) is used for sending and receiving email [5], [6].

One of the key features of TCP/IP is its ability to operate across a variety of different physical network media, including copper wires, fiber optics, and wireless networks. This makes it a flexible and adaptable protocol suite that can be used in a wide range of different environments. Although TCP/IP has been around for several decades, it continues to evolve and improve. For example, IPv6 is a newer version of the IP protocol that offers several improvements over IPv4, including support for more IP addresses and improved security features.

Overall, TCP/IP is a critical protocol suite that underpins the modern Internet and enables communication between devices around the world. Its openness, flexibility, and extensibility have enabled the development of a wide range of new applications and services, and it will likely continue to play a key role in the evolution of the Internet in the years to come. The TCP/IP protocol suite is a set of communication protocols that are used to establish and maintain network connectivity between devices on the Internet. The protocol suite consists of two main protocols: the Transmission Control Protocol (TCP) and the Internet Protocol (IP). The Internet Protocol (IP) is responsible for the routing and delivery of data packets between devices on the Internet. It is a connectionless protocol, which means that it does not establish a dedicated connection between devices before transmitting data. Instead, data packets are transmitted independently and are reassembled at the receiving device based on information in the packet header.

DISCUSSION

The TCP protocol, on the other hand, is responsible for ensuring that data packets are transmitted reliably and in the correct order. It establishes a dedicated connection between devices before transmitting data and uses a variety of mechanisms to ensure that data is delivered without errors. These mechanisms include checksums, acknowledgements, and retransmission of lost packets. Other protocols that are part of the TCP/IP protocol suite include the User Datagram Protocol (UDP), which is a connectionless protocol similar to IP but with a simpler design, and the Internet Control Message Protocol (ICMP), which is used to exchange error messages and diagnostic information between devices on the Internet [7].The TCP/IP protocol suite also includes a number of application-layer protocols that are used for specific purposes. These include protocols such as the Hypertext Transfer Protocol (HTTP), which is used to transmit data over the World Wide Web, the Simple Mail Transfer Protocol (SMTP), which is used for email

transmission, and the File Transfer Protocol (FTP), which is used for file transfers.In order to understand how the TCP/IP protocol suite works, it is helpful to understand the different layers of the protocol stack. The TCP/IP protocol stack is organized into four layers: the application layer, the transport layer, the network layer, and the data link layer.

The application layer is responsible for providing specific services to users, such as web browsing, email, or file transfer. This layer interacts directly with the user and with application programs running on the user's device. The transport layer is responsible for providing reliable data transfer between devices. This layer is primarily concerned with the TCP and UDP protocols, which handle the transmission and receipt of data packets. The network layer is responsible for routing data between devices on the Internet. This layer interacts with the IP protocol to determine the best route for data packets to travel between devices [8] .

Finally, the data link layer is responsible for transmitting data over physical networks, such as Ethernet or Wi-Fi. This layer interacts with the network interface card (NIC) on the user's device to transmit data packets over the physical network. Each layer of the TCP/IP protocol stack interacts with the layer above and below it in a specific way. For example, when data is transmitted from the application layer to the transport layer, it is first encapsulated in a TCP or UDP header that includes information about the data payload, the source and destination IP addresses, and other data relevant to the transport layer.

When data is transmitted from the transport layer to the network layer, it is encapsulated in an IP header that includes information about the source and destination IP addresses, the protocol used for the data transmission, and other data relevant to the network layer.At the data link layer, the data is further encapsulated in a frame that includes information about the physical network, such as the MAC address of the sending and receiving devices. When data is received by a device, the opposite process occurs, with each layer of the protocol stack stripping away the headers and data encapsulation until the original data payload is revealed.

One of the key advantages of the TCP/IP protocol suite is its flexibility and extensibility. Because the protocol suite is based on a modular, layered architecture, it is relatively easy to add new protocols and functionality to the protocol suite. This has allowed the Internet to evolve and expand over time, as new protocols have been developed to meet changing needs. Another key advantage of the TCP/IP protocol suite is its scalability. Because the protocol suite is designed to work across a wide range of different network types and sizes, it can be used to connect devices ranging from small home networks to large corporate networks and the entire Internet.

However, the TCP/IP protocol suite is not without its limitations. One of the main challenges with the protocol suite is its lack of built-in security mechanisms. While the protocol suite includes some security protocols, such as the Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols for encrypting data transmissions, these are not universally implemented and can be vulnerable to attacks. Another limitation of the TCP/IP protocol suite is its dependence on the Internet Protocol version 4 (IPv4) addressing scheme. This addressing scheme uses 32-bit addresses, which limits the number of unique IP addresses that can be assigned to devices on the Internet. This has led to the development of the newer Internet Protocol version 6 (IPv6), which uses 128-bit addresses and provides a much larger address space.Despite these limitations, the TCP/IP protocol suite remains a fundamental component of the Internet and is used by millions of devices around the world. Its flexibility, scalability, and extensibility have allowed it to evolve and adapt to changing needs over time, and it is likely to

continue to play a key role in the future of networking and communication. The OSI model was created before the TCPIIP protocol suite. As a result, the layers in the OSI model and the TCP/IP protocol suite do not perfectly correspond. The four levels of the original TCP/IP protocol suite were host-to-network, internet, transport, and application. Yet, when OSI and TCP/IP are contrasted, we may suppose that the physical and data connection layers are combined to form the host-to-network layer. The application layer essentially performs the functions of the session, presentation, and application layers, with the transport layer in TCPIIP handling some of the session layer's responsibilities. The internet layer is analogous to the network layer. The five levels of the TCPIIP protocol suite are thus assumed in this book to be physical, data link, network, transport, and application. According to the first four levels of the OSI model, the first four tiers offer physical standards, network interfaces, internetworking, and transport services. Nevertheless, the application layer in TCPIIP serves as a substitute for the three uppermost levels in the OSI model.

The interactive modules that make up the hierarchical protocol TCP/IP each have a defined job to perform, although they are not always interconnected. The layers of the TCP/IP protocol suite comprise generally independent protocols that may be mixed and matched depending on the requirements of the system, in contrast to the OSI model, which defines which functions belong to each of its levels. Each upper-level protocol is backed by one or more lower-level protocols, which is what is meant by the word "hierarchical." Transmission Control Protocol (TCP), User Datagram Protocol (UDP), and Stream Control Transmission Protocol are the three protocols that TCP/IP specifies at the transport layer (SCTP). The Internetworking Protocol (IP), which is the primary protocol specified by TCP/IP at the network layer, is one of many different protocols that facilitate data transfer in this layer.

The Internetworking Protocol is supported by TCP/IP at the network layer (or, more precisely, the internetwork layer). ARP, RARP, ICMP, and IGMP are the four supporting protocols used by IP. In subsequent Internetworking Protocol versions, each of these protocols is detailed in more depth (IP). The TCP/IP protocols employ the Internetworking Protocol (IP) as their primary communication method. It is a connectionless protocol with a best-effort delivery system. Best effort refers to the absence of error checking or tracking in IP. IP makes every effort to send a communication to its intended location while assuming that the underlying layers are unreliable. Data is sent via IP in packets known as datagrams, each of which is sent independently. Datagrams may take several paths, arrive out of order, or even be duplicated. As soon as a datagram reaches its destination, it cannot be reordered since IP does not maintain track of the paths. Yet, IP's restricted capability shouldn't be seen as a flaw. IP offers basic transmission capabilities, freeing the user to add just the features required for a particular application and enabling optimal efficiency.

A logical address is connected to a physical address via the Address Resolution Protocol (ARP). Each device on a connection on a conventional physical network, such a LAN, is identifiable by a physical or station address, which is often written on the network interface card (NIC). When a node's Internet address is known, ARP is used to determine the node's physical address. When a host just knows its physical address, the Reverse Address Resolution Protocol (RARP) enables it to get its Internet address. It is used when a diskless computer boots up or when a machine is connected to a network for the first time. RARP is covered. A technique used by hosts and gateways to notify the sender of datagram issues is the Internet Control Message Protocol (ICMP). Query and error reporting messages are sent through ICMP.

The simultaneous sending of a message to a number of receivers is made possible via the Internet Group Message Protocol (IGMP). TCP and UDP were the two protocols that were formerly used to represent the transport layer in TCP/IP. Due to the fact that IP is a host-to-host protocol, it may transmit a packet from one physical device to another. Transport level protocols UDP and TCP are in charge of sending messages from one process (running software) to another process. SCTP, a new transport layer protocol, was developed to accommodate certain more recent uses.

The easier of the two TCPIIP transport standards is the User Datagram Protocol (UDP). It is a process-to-process protocol that merely augments the data from the higher layer with port addresses, checksum error control, and length information. Applications are given full access to transport-layer services using the Transmission Control Protocol (TCP). A trustworthy stream transfer protocol is TCP. In this usage, the word "stream" refers to a connection-oriented system: Before either end of a transmission may send data, a link between the two ends is required. Each transmission's sending end uses TCP to segment the stream of data into smaller pieces known as segments. Together with an acknowledgement number for the segments received, each segment comes with a sequence number for later reordering. Inside of IP datagrams, segments are sent through the internet. TCP gathers each datagram as it arrives at the receiving end and reorders the transmission according to the sequence numbers.

Newer applications like telephony over the Internet are supported via the Stream Control Transmission Protocol (SCTP). The greatest aspects of UDP and TCP are combined in this transport layer protocol. The combined session, presentation, and application layers in the OSI model are identical to the application layer in TCPIIP. At this layer, several protocols are specified. Further chapters address many of the common protocols. The address of a node as specified by its LAN or WAN is the physical address, commonly referred to as the link address. It is a part of the frame that the data link layer employs. The lowest level address is this one.

On the network, the physical addresses are in charge (LAN or WAN). Depending on the network, these addresses might have different sizes and formats. For instance, the network interface card's imprinted 6-byte (48-bit) physical address is used by Ethernet (NIC). Nevertheless, the I-byte dynamic address used by Local Talk (Apple) varies each time the station launches. Universal communications that are not reliant on underlying physical networks need logical addresses. In an environment where multiple networks may have distinct address formats, physical addresses are inadequate. No of the underlying physical network, each host must be able to be uniquely recognized using a system of universal addressing [9].

The logical addresses were created with this in mind. On the Internet today, a logical address is a 32-bit identifier that may specifically identify a host connected to the network. On the Internet, no two publicly addressed and accessible hosts may have the same IP address. A packet has to be sent from the computer with the logical address A and physical address 10 to the computer with the logical address P and physical address. We employ letters to represent logical addresses and numbers to represent physical addresses; but, as we shall learn later in the chapter, both are essentially numbers.

At the network layer, the sender encodes its data in a packet and adds two logical addresses (A and P). Keep in mind that the logical source address often precedes the logical destination address in most protocols (contrary to the order of physical addresses). Before the packet can be sent, however, the network layer must determine the physical address of the next hop. The network layer looks for the next hop's logical address (router I) in its routing table, and it

discovers that it is F. The physical address of router 1 that matches to the logical address of 20 is discovered using the ARP explained above. The data link layer then receives this address from the network layer and wraps the packet with the physical source address 10 and the physical destination address 20.

Every device on LAN 1 receives the frame, but all of them ignore it save router 1, which determines that the destination physical address in the frame corresponds with its own physical address. For the purpose of reading the logical destination address P, the router decapsulates the packet from the frame. The router is aware that the packet has to be forwarded since the logical destination address does not correspond to the router's logical address. Addressing router prepares a new frame, wraps the packet, and delivers it to router 2 after consulting its routing table and ARP to determine the physical destination address of the next hop (router 2).

The addresses in the frame should be noted. The physical address of the source shifts from 10 to 99. Router 1's physical address 20 is replaced with 33 as the destination physical address router 2 physical address. The packet will be lost if the logical source and destination addresses are changed. After changing the physical addresses, a new frame is delivered to the target machine. The packet is encapsulated when the frame gets to its final location. The computer's logical address and the target logical address P are identical. Data are delivered to the top layer after being encapsulated from the packet. It should be noted that although logical addresses vary from source to destination, physical addresses do not. Later in the book, we learn that this rule has a few exceptions.

A certain amount of data must go from a source to a destination host, and this requires both the IP address and the physical address. The goal of data transmission via the Internet is not always to reach the target site. A system is incomplete if it just transmits data between computers. Computers of today are machines that can execute many processes at once. A process interacting with another process is the goal of Internet communication. For instance, TELNET may be used to connect computer A and computer C. Computer A and Computer B converse simultaneously using the File Transfer Protocol (FTP). We need a technique to identify the various processes in order for them to receive data concurrently.

They thus need addresses. The label given to a process in the TCPIIP architecture is referred to as a port address. In TCPIIP, a port address is 16 bits long. In addition to the protocols already mentioned, the TCP/IP protocol suite also includes a number of other important protocols, such as the Address Resolution Protocol (ARP) and the Reverse Address Resolution Protocol (RARP), which are used to map network addresses to physical addresses and vice versa. The Internet Group Management Protocol (IGMP) is used for managing multicast group memberships, and the Border Gateway Protocol (BGP) is used for exchanging routing information between different autonomous systems on the Internet.

Another important protocol is the Domain Name System (DNS), which is used to translate human-readable domain names, into IP addresses that can be used by the underlying TCP/IP protocols. DNS is an essential part of the Internet infrastructure, and its operation is critical to the functioning of many applications and services on the Internet. In addition to these core protocols, the TCP/IP protocol suite also includes a number of other protocols that are used for specific purposes. For example, the Simple Network Management Protocol (SNMP) is used for managing and monitoring network devices, while the Lightweight Directory Access Protocol (LDAP) is used for accessing and managing directory services.

CONCLUSION

The TCP/IP Protocol Suite is a set of communication protocols that provides the foundation for communication over the Internet and other computer networks. It is organized into layers that perform specific functions, and it includes protocols like TCP, IP, and UDP that are responsible for reliable and efficient data transfer [10], [11] . TCP/IP is an open and extensible protocol suite that has enabled the development of many new applications and services, and it can operate across a wide range of different physical network media. Despite being several decades old, TCP/IP continues to evolve and improve, and it will likely remain a critical protocol suite that underpins the modern Internet for many years to come.

REFERENCES

[1] A. Tyagi, "TCP/IP Protocol Suite," *Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol.*, 2020, doi: 10.32628/cseit206420.

[2] S. M. Bellovin, "Security problems in the TCP/IP protocol suite," *ACM SIGCOMM Comput. Commun. Rev.*, 1989, doi: 10.1145/378444.378449.

[3] S. Steinke, "The TCP/IP Protocol Suite," in *Network Tutorial*, 2020. doi: 10.1201/9781482280876-41.

[4] C. H. Rowland, "Covert channels in the TCP/IP protocol suite," *First Monday*, 1997, doi: 10.5210/fm.v2i5.528.

[5] A. Kumar and S. Karthikeyan, "Security Model for TCP/IP Protocol Suite," *J. Adv. Inf. Technol.*, 2011, doi: 10.4304/jait.2.2.87-91.

[6] A. Tyagi, "TCP / IP Protocol Suite and IP Addressing," *J. Sci. Res. Comput. Sci. Eng. Inf. Technol.*, 2020.

[7] S. M. Bellovin, "A look back at 'security problems in the TCP/IP protocol suite,'" in *Proceedings - Annual Computer Security Applications Conference, ACSAC*, 2004. doi: 10.1109/csac.2004.3.

[8] S. Kent, "Comments on 'security problems in the TCP/IP protocol suite,'" *ACM SIGCOMM Comput. Commun. Rev.*, 1989, doi: 10.1145/74674.74675.

[9] K. Iniewski, C. McCrosky, and D. Minoli, "TCP/IP Protocol Suite," in *Network Infrastructure and Architecture*, 2008. doi: 10.1002/9780470253526.ch5.

[10] W. N. Wang and Z. Zhou, "TCP/IP protocol suite as complex networks," *Nanjing Youdian Xueyuan Xuebao/Journal Nanjing Inst. Posts Telecommun.*, 2005.

[11] A. Epishkina, M. Finoshin, and K. Kogos, "Information Science and Applications (ICISA) 2016," *Lect. Notes Electr. Eng.*, 2016.

CHAPTER 5

PHYSICAL LAYER AND MEDIA: AN ANALYSIS OF THE FUNDAMENTALS, CHALLENGES, AND ADVANCEMENTS IN DATA COMMUNICATION TECHNOLOGIES

Dr. Deepak Chauhan, Assistant Professor,
Department of Computer Science, Sanskriti University, Mathura, Uttar Pradesh, India,
Email id- deepak.chauhan@sanskriti.edu.in

ABSTRACT:

The media used in communication can be classified as either guided or unguided. Guided media includes copper cables, fiber optic cables, and twisted pair cables, while unguided media includes wireless transmission methods such as radio waves, microwaves, and infrared signals. The choice of medium used in a communication system is dependent on a variety of factors including cost, bandwidth, and the distance between the communicating devices. The physical layer is critical to the overall performance of a communication system, as it establishes the foundation for all subsequent layers to operate effectively. The success of data transmission over a network is highly dependent on the quality of the physical layer and the chosen medium. As such, designing a robust physical layer with an appropriate medium is crucial for the success of any communication system.

KEYWORDS:

Bandwidth, Communication, Media, Fiber Optic, Twisted Cables.

INTRODUCTION

The physical layer is the lowest layer of the OSI model and is responsible for the transmission of data over a communication channel. The physical layer is concerned with the physical transmission of data and is responsible for converting digital data into a format that can be transmitted over a communication medium. The physical layer is also responsible for ensuring that the data is transmitted correctly and that the receiver can decode the data [1]–[3]. The physical layer is responsible for defining the electrical, mechanical, and timing specifications for transmitting data over a communication channel. The physical layer is concerned with the transmission of bits, which are the basic units of digital data. The physical layer specifies how these bits are transmitted over a communication channel, including the type of medium that is used to transmit the data. Media is the means of transmitting data between two devices. Media can be classified into two types: guided and unguided. Guided media are those that use a physical cable to transmit data, while unguided media are those that use wireless signals to transmit data. Some of the most common types of media used for transmitting data are discussed below.

Copper Cable Copper cables are a type of guided media that are commonly used for transmitting data over short distances. Copper cables are available in various types, including twisted pair cable, coaxial cable, and shielded twisted pair cable. Twisted pair cable is commonly used for Ethernet networks and is made up of two or more insulated copper wires that are twisted together. Coaxial cable is commonly used for cable television networks and is made up of a

central conductor surrounded by a shield and an insulating layer. Shielded twisted pair cable is a type of cable that is similar to twisted pair cable, but has an additional layer of shielding to protect against electromagnetic interference. Fiber Optic Cable Fiber optic cable is a type of guided media that is commonly used for transmitting data over long distances. Fiber optic cable is made up of thin strands of glass or plastic that are used to transmit data using light signals. Fiber optic cable is capable of transmitting data at much higher speeds than copper cables and is also more resistant to electromagnetic interference [4].

Wireless Transmission Wireless transmission is a type of unguided media that is commonly used for transmitting data over short distances. Wireless transmission uses electromagnetic waves to transmit data between devices. The most common types of wireless transmission include infrared, Bluetooth, and Wi-Fi. Infrared is commonly used for transmitting data between devices that are in close proximity to each other. Bluetooth is commonly used for transmitting data between devices that are within a few meters of each other. Wi-Fi is commonly used for transmitting data over a larger area, such as within a building or a campus.

Satellite Transmission Satellite transmission is a type of unguided media that is commonly used for transmitting data over long distances. Satellite transmission uses satellites orbiting the Earth to transmit data between devices. Satellite transmission is commonly used for transmitting television signals, as well as for providing internet access in remote areas. The physical layer is responsible for ensuring that data is transmitted correctly and that the receiver can decode the data. To achieve this, the physical layer uses various techniques, including encoding, modulation, and multiplexing.

Encoding is the process of converting digital data into a format that can be transmitted over a communication channel. Encoding is necessary because the digital data that is transmitted over a communication channel needs to be converted into a format that can be understood by the physical layer. Some of the most common encoding techniques used by the physical layer include Manchester encoding, differential Manchester encoding, and 4B/5B encoding. Modulation is the process of changing the characteristics of a signal to transmit information. Modulation is necessary because the signal that is transmitted over a communication channel needs to be changed in order to carry information. Some of the most common modulation techniques used by the physical layer include amplitude modulation, frequency modulation, and phase modulation [5], [6] .

Amplitude modulation is a technique in which the amplitude of a carrier wave is varied to represent the data that is being transmitted. In frequency modulation, the frequency of the carrier wave is varied to represent the data that is being transmitted. In phase modulation, the phase of the carrier wave is varied to represent the data that is being transmitted. Multiplexing is the process of transmitting multiple signals over a single communication channel. Multiplexing is necessary because communication channels have a limited bandwidth, and it is not possible to transmit all signals over a separate channel. Some of the most common multiplexing techniques used by the physical layer include time-division multiplexing (TDM) and frequency-division multiplexing (FDM).

In TDM, multiple signals are transmitted over a single channel by dividing the channel into time slots. Each signal is transmitted during its designated time slot. In FDM, multiple signals are transmitted over a single channel by dividing the channel into frequency bands. Each signal is transmitted in its designated frequency band. The physical layer is also responsible for error

detection and correction. Error detection and correction techniques are used to ensure that data is transmitted correctly and that errors are corrected if they occur during transmission. Some of the most common error detection and correction techniques used by the physical layer include parity checking, cyclic redundancy checking (CRC), and forward error correction (FEC).

Parity checking is a technique in which a parity bit is added to the data that is being transmitted. The parity bit is used to detect errors that occur during transmission. If an error is detected, the data is retransmitted. CRC is a technique in which a checksum is added to the data that is being transmitted. The checksum is used to detect errors that occur during transmission. If an error is detected, the data is retransmitted[7].

FEC is a technique in which redundant data is added to the data that is being transmitted. The redundant data is used to correct errors that occur during transmission. If an error is detected, the redundant data is used to correct the error.

DISCUSSION

The physical layer is the lowest layer of the OSI model and is responsible for the transmission of data over a communication channel. The physical layer is concerned with the physical transmission of data and is responsible for converting digital data into a format that can be transmitted over a communication medium. The physical layer is also responsible for ensuring that the data is transmitted correctly and that the receiver can decode the data. The physical layer is responsible for defining the electrical, mechanical, and timing specifications for transmitting data over a communication channel. The physical layer is concerned with the transmission of bits, which are the basic units of digital data. The physical layer specifies how these bits are transmitted over a communication channel, including the type of medium that is used to transmit the data [8].

Media is the means of transmitting data between two devices. Media can be classified into two types: guided and unguided. Guided media are those that use a physical cable to transmit data, while unguided media are those that use wireless signals to transmit data. Some of the most common types of media used for transmitting data are discussed below. Copper Cable Copper cables are a type of guided media that are commonly used for transmitting data over short distances. Copper cables are available in various types, including twisted pair cable, coaxial cable, and shielded twisted pair cable. Twisted pair cable is commonly used for Ethernet networks and is made up of two or more insulated copper wires that are twisted together. Coaxial cable is commonly used for cable television networks and is made up of a central conductor surrounded by a shield and an insulating layer. Shielded twisted pair cable is a type of cable that is similar to twisted pair cable, but has an additional layer of shielding to protect against electromagnetic interference [9], [10] .

Fiber Optic Cable Fiber optic cable is a type of guided media that is commonly used for transmitting data over long distances. Fiber optic cable is made up of thin strands of glass or plastic that are used to transmit data using light signals. Fiber optic cable is capable of transmitting data at much higher speeds than copper cables and is also more resistant to electromagnetic interference. Wireless Transmission Wireless transmission is a type of unguided media that is commonly used for transmitting data over short distances. Wireless transmission uses electromagnetic waves to transmit data between devices. The most common types of wireless transmission include infrared, Bluetooth, and Wi-Fi. Infrared is commonly used for

transmitting data between devices that are in close proximity to each other. Bluetooth is commonly used for transmitting data between devices that are within a few meters of each other. Wi-Fi is commonly used for transmitting data over a larger area, such as within a building or a campus.

Satellite Transmission Satellite transmission is a type of unguided media that is commonly used for transmitting data over long distances. Satellite transmission uses satellites orbiting the Earth to transmit data between devices. Satellite transmission is commonly used for transmitting television signals, as well as for providing internet access in remote areas.The physical layer is responsible for ensuring that data is transmitted correctly and that the receiver can decode the data. To achieve this, the physical layer uses various techniques, including encoding, modulation, and multiplexing.

Encoding is the process of converting digital data into a format that can be transmitted over a communication channel. Encoding is necessary because the digital data that is transmitted over a communication channel needs to be converted into a format that can be understood by the physical layer. Some of the most common encoding techniques used by the physical layer include Manchester encoding, differential Manchester encoding, and 4B/5B encoding. Modulation is the process of changing the characteristics of a signal to transmit information. Modulation is necessary because the signal that is transmitted over a communication channel needs to be changed in order to carry information. Some of the most common modulation techniques used by the physical layer include amplitude modulation, frequency modulation, and phase modulation. Amplitude modulation is a technique in which the amplitude of a carrier wave is varied to represent the data that is being transmitted. In frequency modulation, the frequency of the carrier wave is varied to represent the data that is being transmitted. In phase modulation, the phase of the carrier wave is varied to represent the data that is being transmitted.

Multiplexing is the process of transmitting multiple signals over a single communication channel. Multiplexing is necessary because communication channels have a limited bandwidth, and it is not possible to transmit all signals over a separate channel. Some of the most common multiplexing techniques used by the physical layer include time-division multiplexing (TDM) and frequency-division multiplexing (FDM). In TDM, multiple signals are transmitted over a single channel by dividing the channel into time slots. Each signal is transmitted during its designated time slot. In FDM, multiple signals are transmitted over a single channel by dividing the channel into frequency bands. Each signal is transmitted in its designated frequency band.

The physical layer is also responsible for error detection and correction. Error detection and correction techniques are used to ensure that data is transmitted correctly and that errors are corrected if they occur during transmission. Some of the most common error detection and correction techniques used by the physical layer include parity checking, cyclic redundancy checking (CRC), and forward error correction (FEC). Parity checking is a technique in which a parity bit is added to the data that is being transmitted. The parity bit is used to detect errors that occur during transmission. If an error is detected, the data is retransmitted.CRC is a technique in which a checksum is added to the data that is being transmitted. The checksum is used to detect errors that occur during transmission. If an error is detected, the data is retransmitted.

FEC is a technique in which redundant data is added to the data that is being transmitted. The redundant data is used to correct errors that occur during transmission. If an error is detected, the redundant data is used to correct the error.As mentioned earlier, media can be classified into two

types: guided and unguided. Guided media are those that use physical cables or wires to transmit data, whereas unguided media use wireless signals to transmit data. Guided media includes various types of cables such as twisted pair cables, coaxial cables, and fiber optic cables. Twisted pair cables consist of a pair of copper wires that are twisted together to reduce interference from other signals. These cables are commonly used for telephone lines, local area networks (LANs), and some wide area networks (WANs).

Coaxial cables consist of a central conductor surrounded by an insulating layer, a metallic shield, and an outer insulating layer. These cables are commonly used for cable television and some high-speed Internet connections. Fiber optic cables consist of thin strands of glass or plastic that use light to transmit data. These cables are commonly used for high-speed Internet connections and some long-distance telecommunications. Unguided media includes various types of wireless signals such as radio waves, microwaves, and infrared waves. Radio waves are commonly used for wireless communications, including cellular phones, Wi-Fi, and Bluetooth devices. Microwaves are used for satellite communications, radar systems, and microwave ovens. Infrared waves are used for short-range wireless communications, including remote controls and some wireless keyboards and mice.

Modulation is the process of modifying a carrier signal to encode information. Some common modulation techniques used by the physical layer include amplitude modulation (AM), frequency modulation (FM), and phase modulation (PM). In amplitude modulation, the amplitude of the carrier signal is varied to represent the data being transmitted. The amplitude of the carrier signal increases or decreases based on the binary value of the data. In frequency modulation, the frequency of the carrier signal is varied to represent the data being transmitted. The frequency of the carrier signal increases or decreases based on the binary value of the data. In phase modulation, the phase of the carrier signal is varied to represent the data being transmitted. The phase of the carrier signal changes based on the binary value of the data.

Multiplexing is the process of transmitting multiple signals over a single communication channel. Some common multiplexing techniques used by the physical layer include time-division multiplexing (TDM) and frequency-division multiplexing (FDM).In TDM, multiple signals are transmitted over a single channel by dividing the channel into time slots. Each signal is transmitted during its designated time slot. In FDM, multiple signals are transmitted over a single channel by dividing the channel into frequency bands. Each signal is transmitted in its designated frequency band. Error detection and correction techniques are used to ensure that data is transmitted correctly and that errors are corrected if they occur during transmission. Some common error detection and correction techniques used by the physical layer include parity checking, cyclic redundancy checking (CRC), and forward error correction (FEC).

In CRC, a checksum is added to the data that is being transmitted. The checksum is used to detect errors that occur during transmission. If an error is detected, the data is retransmitted. In FEC, redundant data is added to the data that is being transmitted. The redundant data is used to correct errors that occur during transmission. If an error is detected, the redundant data is used to correct the error. The physical layer of a communication system is responsible for the transmission of raw data bits over a communication medium. This layer is concerned with the electrical, mechanical, and functional specifications of the physical medium used for communication. The physical layer also defines the rules for transmitting and receiving signals

between devices, including the encoding of data, modulation schemes, error detection and correction, and the synchronization of data transmission.

In this article, we will explore the physical layer and different types of media used in communication. We will discuss the characteristics of guided and unguided media, the advantages and disadvantages of different types of media, and the different transmission technologies used for data communication. We will also discuss the key issues related to the physical layer in data communication and the protocols used to manage the physical layer. The Physical Layer in Data Communication The physical layer is the first layer in the Open Systems Interconnection (OSI) model of communication. This layer is responsible for the transmission of raw bits over a communication medium. The physical layer deals with the physical characteristics of the medium used for communication, including the transmission rate, physical connectors, and physical topologies. The physical layer also includes the transmission of data in the form of electrical or electromagnetic signals.

The physical layer establishes the foundation for all subsequent layers to operate effectively. The success of data transmission over a network is highly dependent on the quality of the physical layer and the chosen medium. As such, designing a robust physical layer with an appropriate medium is crucial for the success of any communication system.Types of Media the media used in communication can be classified as either guided or unguided. Guided media includes copper cables, fiber optic cables, and twisted pair cables, while unguided media includes wireless transmission methods such as radio waves, microwaves, and infrared signals.

Guided Media Copper Cables: Copper cables are the most widely used medium for communication. Copper cables are used for both data communication and voice communication. Copper cables are inexpensive, easy to install, and can be used for short and long-distance communication. Copper cables are also flexible, durable, and resistant to interference. There are two types of copper cables used in data communication, twisted-pair cables and coaxial cables. Twisted-pair cables consist of two insulated wires twisted together. These cables are used for short-distance communication and are inexpensive. Coaxial cables consist of a central conductor and an outer conductor. These cables are used for longer distance communication and are more expensive than twisted-pair cables.

Fiber Optic Cables: Fiber optic cables are used for high-speed data communication. These cables consist of a core made of glass or plastic surrounded by a cladding material that reflects light back into the core. Fiber optic cables are used for long-distance communication and have a higher bandwidth than copper cables. Fiber optic cables are also immune to electromagnetic interference. Fiber optic cables are expensive and require specialized equipment for installation and maintenance. However, fiber optic cables are increasingly being used in communication systems due to their high-speed and reliability.

Twisted pair cables are used for both data and voice communication. These cables consist of two insulated wires twisted together. Twisted pair cables are inexpensive and can be used for short distance communication. The twisted pairs in these cables help reduce the electromagnetic interference. Radio waves are used for wireless communication. These waves have a high frequency and are used for communication over long distances. Radio waves are used for communication between radio and television stations, cell phones, and satellite communication. Microwaves are used for communication over short distances. These waves are used for communication between buildings, microwave ovens, and in the radar systems. Microwaves

have a higher frequency than radio waves.Infrared signals are used for short-range communication. These signals are used in remote controls, medical devices, and security systems. Infrared signals have a lower frequency than microwaves and cannot penetrate walls.

Copper cables are inexpensive, easy to install, and can be used for short and long-distance communication. Copper cables are also flexible, durable, and resistant to interference. However, copper cables have a limited bandwidth and are susceptible to electromagnetic interference. Fiber optic cables have a high bandwidth and are immune to electromagnetic interference. These cables are also used for long-distance communication. However, fiber optic cables are expensive and require specialized equipment for installation and maintenance. Twisted pair cables are inexpensive and can be used for short-distance communication. However, twisted pair cables have a limited bandwidth and are susceptible to electromagnetic interference. Radio waves have a high frequency and are used for communication over long distances. Radio waves are used for communication between radio and television stations, cell phones, and satellite communication. However, radio waves can be affected by interference and have a limited bandwidth [11].

Microwaves are used for communication over short distances. These waves have a higher frequency than radio waves, but are still susceptible to interference. Infrared signals are used for short-range communication. These signals are used in remote controls, medical devices, and security systems. However, infrared signals have a limited range and cannot penetrate walls. In analog transmission, the signal is transmitted as a continuous wave. This type of transmission is used for voice communication and has a low bandwidth. Digital Transmission: In digital transmission, the signal is transmitted as a series of discrete bits. This type of transmission is used for data communication and has a higher bandwidth than analog transmission. Modulation is the process of encoding data onto a carrier signal. Modulation is used to transmit data over different types of media, including copper cables, fiber optic cables, and wireless communication.

Multiplexing is the process of combining multiple signals into a single signal. This process is used to increase the efficiency of communication over a medium. The physical layer is critical to the overall performance of a communication system. The physical layer is responsible for the transmission of raw bits over a communication medium. The success of data transmission over a network is highly dependent on the quality of the physical layer and the chosen medium[12], [13]. Signal attenuation is the loss of signal strength as the signal travels over a medium. Signal attenuation can result in a degradation of the signal and affect the quality of communication. Interference is the presence of unwanted signals that can affect the quality of communication. Interference can be caused by electromagnetic interference or radio-frequency interference. Noise is the unwanted signal that is introduced into a communication system. Noise can be caused by interference or signal attenuation.

Used to Manage the Physical Layer Different protocols are used to manage the physical layer in data communication. Ethernet is a protocol used for wired communication. This protocol is used to manage the physical layer and the data link layer in a communication system.Wi-Fi is a protocol used for wireless communication. This protocol is used to manage the physical layer and the data link layer in a wireless communication system.Bluetooth is a protocol used for short-range wireless communication. This protocol is used to manage the physical layer and the data link layer in a wireless communication system.ZigBee is a protocol used for low-power

wireless communication. This protocol is used to manage the physical layer and the data link layer in a wireless communication system.

CONCLUSION

The physical layer is responsible for the transmission of data over a communication channel. The physical layer is concerned with the physical transmission of data and is responsible for converting digital data into a format that can be transmitted over a communication medium. The physical layer is also responsible for ensuring that the data is transmitted correctly and that the receiver can decode the data. Media is the means of transmitting data between two devices, and it can be classified into two types: guided and unguided. The physical layer uses various techniques, including encoding, modulation, and multiplexing, to ensure that data is transmitted correctly. Error detection and correction techniques are also used by the physical layer to ensure that errors are corrected if they occur during transmission.

REFERENCES

[1] C. B. Mwakwata, H. Malik, M. M. Alam, Y. Le Moullec, S. Parand, and S. Mumtaz, "Narrowband internet of things (NB-IoT): From physical (PHY) and media access control (MAC) layers perspectives," *Sensors (Switzerland)*, 2019, doi: 10.3390/s19112613.

[2] S. Climent, A. Sanchez, J. V. Capella, N. Meratnia, and J. J. Serrano, "Underwater acousticwireless sensor networks: Advances and future trends in physical, MAC and routing layers," *Sensors (Switzerland)*, 2014, doi: 10.3390/s140100795.

[3] N. Xie, Z. Li, and H. Tan, "A Survey of Physical-Layer Authentication in Wireless Communications," *IEEE Communications Surveys and Tutorials*. 2021. doi: 10.1109/COMST.2020.3042188.

[4] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Commun. Surv. Tutorials*, 2014, doi: 10.1109/SURV.2014.012314.00178.

[5] T. Kim, I. H. Kim, Y. Sun, and Z. Y. Jin, "Physical layer and medium access control design in energy efficient sensor networks: An overview," *IEEE Trans. Ind. Informatics*, 2015, doi: 10.1109/TII.2014.2379511.

[6] R. Melki, H. N. Noura, M. M. Mansour, and A. Chehab, "A survey on OFDM physical layer security," *Phys. Commun.*, 2019, doi: 10.1016/j.phycom.2018.10.008.

[7] S. Madhu, M. Bal Raju, and P. Chenna Reddy, "Enhancing transport of media using physical layer based approach," *Int. J. Appl. Eng. Res.*, 2017.

[8] Y. Liu, H. H. Chen, and L. Wang, "Physical Layer Security for Next Generation Wireless Networks: Theories, Technologies, and Challenges," *IEEE Commun. Surv. Tutorials*, 2017, doi: 10.1109/COMST.2016.2598968.

[9] J. S. Wey *et al.*, "Physical layer aspects of NG-PON2 standards - Part 1: Optical link design [Invited]," *J. Opt. Commun. Netw.*, 2016, doi: 10.1364/JOCN.8.000033.

[10] IEEE Computer Society, "Part 11: Wireless Lan Medium Access Control (MAC) and Physical Layer (PHY) Specifications," *IEEE Std 802.11-2007*, 2007.

[11] L. Oliveira, J. J. P. C. Rodrigues, S. A. Kozlov, R. A. L. Rabêlo, and V. H. C. de Albuquerque, "MAC layer protocols for internet of things: A survey," *Future Internet*. 2019. doi: 10.3390/fi11010016.

[12] A. M. Tonello, N. A. Letizia, D. Righini, and F. Marcuzzi, "Machine Learning Tips and Tricks for Power Line Communications," *IEEE Access*, 2019, doi: 10.1109/ACCESS.2019.2923321.

[13] C. Cano, A. Pittolo, D. Malone, L. Lampe, A. M. Tonello, and A. G. Dabak, "State of the Art in Power Line Communications: From the Applications to the Medium," *IEEE J. Sel. Areas Commun.*, 2016, doi: 10.1109/JSAC.2016.2566018.

CHAPTER 6

DATA AND SIGNALS: A COMPREHENSIVE STUDY ON THE FUNDAMENTALS AND APPLICATIONS OF DIGITAL COMMUNICATION

Dr. Narendra Kumar Sharma, Assistant Professor,
Department of Computer Science, Sanskriti University, Mathura, Uttar Pradesh, India,
Email id- narendra@sanskriti.edu.in

ABSTRACT:

Data and signals are fundamental components of digital communication systems, responsible for the transmission and reception of information over various communication channels.

This research paper provides a comprehensive study on the fundamentals and applications of digital communication, including the basics of data and signals, encoding and decoding techniques, error detection and correction, and modulation and demodulation schemes. It explores the various types of signals used in digital communication, such as analog and digital signals, and the various communication protocols used in modern communication systems, such as TCP/IP, Ethernet, and Wi-Fi.

KEYWORDS:

Amplitude Modulation, Data, Digital Communication, Frequency, Phase Modulation.

INTRODUCTION

In the field of telecommunications and computer networking, data and signals play an essential role in transmitting information from one point to another. Data refers to any information that is to be communicated, such as text, audio, or video, while signals are the physical representations of this data, such as electrical, electromagnetic, or optical signals. In this article, we will explore the concept of data and signals in greater detail, including their properties, types, and applications [1]–[3].

Data can be described by several properties, including the following:

1. **Information content:** The information content of data refers to the amount of information conveyed by the data. For example, a text message containing a single word has less information content than a paragraph containing multiple sentences.
2. **Structure:** The structure of data refers to the way in which the data is organized or formatted. For example, data may be structured as a database or a file format, such as a text file or an image file.
3. **Modality:** The modality of data refers to the sensory modalities involved in generating and interpreting the data. For example, data may be visual, auditory, or haptic.
4. **Complexity:** The complexity of data refers to the level of detail and the number of parameters involved in describing the data. For example, a high-resolution image has a greater level of complexity than a low-resolution image.

There are several types of data, including the following:

1. **Analog Data:**Analog data is continuous in nature and can take any value within a range. For example, temperature and sound waves are analog data.
2. **Digital Data:**Digital data is discrete in nature and can take only a limited number of values. For example, binary data represented by 0s and 1s is digital data.
3. **Continuous Data:**Continuous data is data that can take any value within a range. For example, temperature is continuous data.
4. **Discrete Data:**Discrete data is data that can take only a limited number of values. For example, the number of students in a classroom is discrete data.
5. **Categorical Data:**Categorical data is data that is divided into categories or classes. For example, hair color is categorical data.

Signals can be described by several properties, including the following:

1. **Amplitude:** The amplitude of a signal refers to its strength or intensity.
2. **Frequency:** The frequency of a signal refers to the number of cycles per second.
3. **Phase:** The phase of a signal refers to the position of the signal in its cycle.
4. **Wavelength:** The wavelength of a signal refers to the distance between two peaks or two troughs.
5. **Period:** The period of a signal refers to the time taken for one complete cycle.

Types of Signals

There are several types of signals, including the following:

1. **Analog signals:** Analog signals are continuous in nature and can take any value within a range. For example, a sound wave is an analog signal.
2. **Digital signals:** Digital signals are discrete in nature and can take only a limited number of values. For example, binary signals represented by 0s and 1s are digital signals.
3. **Periodic signals:** Periodic signals are signals that repeat themselves over time. For example, a sine wave is a periodic signal.
4. **Non-periodic signals:** Non-periodic signals are signals that do not repeat themselves over time. For example, a random noise signal is a non-periodic signal.

Applications of Data and Signals

Data and signals have numerous applications in various fields, including the following:

1. **Telecommunications:** In telecommunications, data and signals are used to transmit information over long distances. For example, telephone calls and internet data are transmitted using data and signals

2. **Computer networking:** In computer networking, data and signals are used to transfer information between computers or devices. For example, emails, web pages, and files are transferred using data and signals.
3. **Audio and video processing:** In audio and video processing, data and signals are used to represent and process audio and video information. For example, digital audio and video files are represented as digital signals.
4. **Medical imaging:** In medical imaging, data and signals are used to represent and process medical images, such as X-rays, CT scans, and MRI scans. These images are represented as digital signals that can be processed by computer algorithms.
5. **Control systems:** In control systems, data and signals are used to monitor and control various processes, such as temperature control, traffic control, and robotics. The sensors and actuators used in control systems generate and process signals that are used to control the system.
6. **Robotics:** In robotics, data and signals are used to control the movement and actions of robots. Sensors on the robot generate signals that are processed by the robot's control system to determine the robot's actions.
7. **Automotive systems:** In automotive systems, data and signals are used to control various aspects of the vehicle, such as engine performance, safety systems, and entertainment systems. The sensors and control systems in the vehicle generate and process signals that are used to control these systems.

DISCUSSION

In the context of digital communication, data is typically converted into a series of binary digits, known as bits, which can be transmitted as a signal through a physical medium, such as a wire or fiber optic cable. The signal can be modulated using various techniques, such as amplitude modulation (AM), frequency modulation (FM), or phase modulation (PM), to encode the information and ensure its reliable transmission [4]. The transmission and reception of signals are subject to various forms of noise and interference, which can corrupt the information being transmitted. To mitigate this, various techniques, such as error-correcting codes and signal processing algorithms, can be employed to improve the signal-to-noise ratio and enhance the reliability of the communication.

Overall, data and signals play a critical role in modern communication and information technology, facilitating the transmission and processing of vast amounts of information across diverse applications and industries. Data and signals are two key concepts in communication systems and information technology. While they are often used interchangeably, they are distinct concepts that are fundamental to understanding how information is transmitted, processed, and analyzed in modern systems. In this article, we will explore the concepts of data and signals, how they are related, and their roles in modern communication and information technology.

Data refers to any collection of facts, figures, or statistics that are to be processed or analyzed to extract meaningful information. Data can be in any form, such as text, numbers, images, videos, or sounds. It can be structured, such as in a database or spreadsheet, or unstructured, such as in a text document or social media post [5].

In the digital age, data is often stored in electronic form, such as in computer files, databases, or cloud storage. This has led to an explosion of data, with organizations and individuals generating and collecting vast amounts of data every day. This data can be analyzed using various techniques, such as data mining, machine learning, and artificial intelligence, to extract insights and make informed decisions. A signal is a physical representation of data that is transmitted through a communication channel. Signals can take many forms, such as electrical, optical, or electromagnetic waves. The transmission of signals can be either analog or digital. An analog signal is a continuous wave that varies in amplitude, frequency, or phase, while a digital signal is a series of discrete bits that represent data in binary form. Signals are used to transmit information over longer distances, such as between devices or over networks. Signals can be modulated to carry information, using techniques such as amplitude modulation (AM), frequency modulation (FM), or phase modulation (PM). This modulation enables the signal to carry information and enables the receiver to demodulate the signal to extract the data.

Analog signals are continuous waves that vary in amplitude, frequency, or phase. Analog signals are used in many applications, such as audio and video transmission, and are often converted into digital form for storage and processing. The transmission of analog signals can be affected by noise and distortion, which can degrade the quality of the signal and lead to errors in transmission. One common example of an analog signal is a sound wave. In audio transmission, the sound wave is captured by a microphone, which converts the sound wave into an electrical signal. The electrical signal is then transmitted over a communication channel, such as a wire or wireless network, and received by a speaker, which converts the electrical signal back into a sound wave [6].

Digital signals are discrete bits that represent data in binary form. Digital signals are used in many applications, such as computer networking, digital audio and video transmission, and digital storage. Digital signals are more resistant to noise and distortion than analog signals, as they can be encoded with error-correcting codes and other techniques that enhance their reliability. In digital communication, data is typically encoded as a series of bits, which are then transmitted as a digital signal over a communication channel. The signal can be modulated using various techniques, such as amplitude shift keying (ASK), frequency shift keying (FSK), or phase shift keying (PSK), to encode the data and ensure its reliable transmission.

The transmission of signals is subject to various forms of noise and interference, which can corrupt the information being transmitted. Noise can come from various sources, such as electromagnetic interference (EMI), radio frequency interference (RFI), or crosstalk from other signals. To mitigate the effects of noise and interference, various techniques can be employed, such as: Error-correcting codes: These are codes that can detect and correct errors in the received signal. Examples of error-correcting codes include parity check codes, cyclic redundancy check (CRC) codes, and forward error correction (FEC) codes are algorithms that can filter out noise and interference from the received signal. Examples of signal processing algorithms include equalizers, adaptive filters, and echo cancellers.

These are techniques that can modulate the signal to make it more resistant to noise and interference. Examples of modulation techniques include quadrature amplitude modulation (QAM), differential phase shift keying (DPSK), and frequency hopping spread spectrum (FHSS). In addition to these techniques, other factors can affect the transmission of signals, such as the bandwidth of the communication channel, the distance between the sender and receiver, and the

power of the transmitter [7]. To ensure reliable and efficient transmission of signals, various standards and protocols have been developed, such as Ethernet, WI-Fi, and Bluetooth.

Data and signals are used in various telecommunications applications, such as voice and video communication, mobile networking, and satellite communication. Data and signals are the foundation of the internet, enabling the transmission of data packets over a global network of interconnected devices. Data and signals are used in various computing applications, such as storage, processing, and transmission of data between devices.

Data and signals are used in various media applications, such as audio and video recording, transmission, and playback. Data and signals are used in various industrial applications, such as process control, monitoring, and optimization.

Data and signals are used in various healthcare applications, such as medical imaging, patient monitoring, and telemedicine. Data and signals are used in various financial applications, such as stock trading, risk management, and fraud detection. One of the key challenges in the field of data and signals is the ever-increasing amount of data being generated and transmitted across networks. This has led to the development of new technologies and standards that can support higher data rates and bandwidths, such as 5G wireless networks and fiber-optic communication systems.

Another challenge is the need for data and signals to be secure and protected from unauthorized access and interference. Encryption and authentication techniques are used to protect data and signals from cyber threats and attacks. In addition, the field of data and signals is constantly evolving, with new technologies and applications emerging all the time [8]. For example, the development of the Internet of Things (IoT) has created new challenges and opportunities for the transmission and processing of data and signals across networks of interconnected devices. The data and signals are foundational concepts in modern communication and information technology, and they will continue to play a critical role in shaping the future of our digital world.

As the field continues to evolve, it will be important to develop new techniques and standards that can support the efficient, reliable, and secure transmission and processing of information. The physical layer's ability to transmit electromagnetic signals carrying data over a transmission channel is one of its main roles. You are dealing with the transfer of data over network connections whether you are gathering numerical information from another computer, delivering animated graphics from a design workstation, or making a bell ring at a remote control centre. The majority of the time, data that is useful to a person or application is not in a format that can be sent across a network. For instance, a picture has to be transformed into a format that transmission medium can use. Transmission medium function by physically guiding energy along a route. Both the signals that indicate data and the data itself may have either an analogue or digital form.

Data might be digital or analogue. Information that is continuous is referred to as analogue data, whereas information with discrete states is referred to as digital data. For instance, a continuous type of information is provided by an analogue clock with hour, minute, and second hands because the motions of the hands are continuous. A digital clock that displays the hours and minutes, on the other hand, will abruptly shift from 8:05 to 8:06. Continuous values may be applied to analogue data, such as the sounds produced by a human voice. An analogue wave is

generated in the air whenever someone talks. This may be either sampled and transformed to a digital signal by a digital signal converter or by a microphone and converted to an analogue signal [9].

Discrete values may be found in digital data. As an example, data are stored in computer memory as Os and 1s. For transmission via a media, they may be modulated into an analogue signal or changed into a digital signal. Signals may be analogue or digital, much like the data they represent. Throughout time, an analogue signal may have an endless number of degrees of intensity. There are an endless number of values along the wave's path as it travels from value A to value B. On the other hand, there are a finite number of specified values for a digital signal. Although each value might be any integer, it is often as simple as 1 and 0.

Plotting signals on two perpendicular axes is the most basic technique to display them. The value or intensity of a signal is shown on the vertical axis. Time is represented via the horizontal axis. A digital signal and an analogue signal, respectively. There are infinity of points that the curve that represents the analogue signal travels through. Yet, the digital signal's vertical lines show how the signal abruptly switches from one value to another. There are two types of analogue and digital signals: periodic and no periodic (sometimes refer to as aperiodic, because the prefix an in Greek means "non"). In a defined amount of time, known as a period, a periodic signal completes a pattern and then repeats that pattern across consecutive similar periods. A cycle is the result of one whole pattern being completed. A no periodic signal fluctuates over time without displaying a pattern or cycle that repeats [10] .

Signals may either be periodic or no periodic in analogue and digital formats. Periodic analogue signals are often used in data transmission because they need less capacity, Periodic analogue signals fall into the simple or composite categories. A sine wave, a straightforward periodic analogue signal, cannot be broken down into simpler signals. A composite sine wave is an analogue periodic signal made up of many sine waves. The most basic kind of periodic analogue signal is the sine wave. The change it undergoes over the course of a cycle is smooth and steady, a continuous, rolling flow, when we think of it as a straightforward oscillating curve. A single arc above the time axis and a single arc below it make up each cycle. We already know that a wave's frequency is the number of cycles it completes in one second and that frequency is the connection between a signal and time. Yet another approach to consider frequency is as a gauge of change pace. As oscillating waveforms, electromagnetic waves continually and predictably vary above and below a mean energy level. As a 40-Hz signal has half the frequency of an 80-Hz signal and completes one cycle in half the time, each cycle's transition from the lowest to the highest voltage levels likewise takes twice as long. Hence, although being expressed in cycles per second (Hz), frequency is a generic measurement of the rate at which a signal changes in relation to time.

The pace of change with regard to time is known as frequency. Change occurs often when it happens quickly. Long-term change indicates low frequency. A signal's frequency is high if the value of the signal fluctuates over a relatively brief period of time. Its frequency is low if it varies slowly over an extended period of time.What happens if a signal remains unchanged? What if it keeps the voltage at the same level the whole time it is active? Its frequency is 0 in this scenario. This concept is easy to understand conceptually. A signal's frequency is aHz if it never completes a cycle and never changes at all.

What happens, however, if a signal changes instantly? What if it quickly moves from one level to another? Then, it has an infinite frequency. While frequency is the inverse of period, in this scenario the frequency is 1/0, or infinite, meaning that when a signal changes instantly, its period is zero (unbounded). Another feature of a signal passing across a transmission medium is its wavelength. A basic sine wave's period or frequency is tied to the medium's propagation speed by its wavelength.

The wavelength of a signal relies on both the frequency and the medium, while the frequency of a signal is independent of the medium. Every signal has a characteristic called a wavelength. The term wavelength is often used in data communications to describe how light travels through an optical cable. The distance a simple signal may cover in one time is known as the wavelength.

If one knows the signal's duration and propagation speed (the speed of light), one may compute the wavelength. Yet, since period and frequency are connected to one another, if we substitute A for wavelength, c for light-speed propagation, and 1 for frequency, we obtain. • Propagation velocity Wavelength = propagation velocity times per second frequency the medium and the signal's frequency both affect how quickly electromagnetic waves spread. For instance, light moves at a speed of 3 x 108 mls in a vacuum. In the case of cable, that speed is significantly lower.

For instance, the wavelength of red light in air is 8 c 3xlO -6 A= - = =0.75 x 10 m=0.75!J.m f 4x 1014 (frequency = 4 x 1014). Nevertheless, the wavelength in a coaxial or fiber-optic connection is shorter (0.5! Jm) due to the cable's slower propagation rate. The amplitude, frequency, and phase together provide a complete definition of a sine wave. Using a technique known as a time-domain plot, we have been demonstrating a sine wave. The amplitude-versus-time graphic in the time-domain displays variations in signal amplitude with respect to time. An implicit phase is not shown on a time-domain graphic.

A frequency-domain diagram may be used to illustrate the connection between amplitude and frequency. The only variables that matter in a frequency-domain display are the peak value and frequency. A period's worth of amplitude changes are not shown. We have been concentrating on basic sine waves thus far.

There are several uses for simple sine waves in everyday life. A single sine wave may be sent to move electrical energy from one location to another. For instance, to provide homes and businesses with electricity, the power company delivers a single sine wave at a frequency of 60 Hz. Another example is to utilise a single sine wave to alert a security centre whenever a home burglar opens a window or door. The sine wave is an energy carrier in the first scenario and a warning indication in the second.

That wouldn't make sense and wouldn't communicate any information if we could just transmit one sine wave throughout a phone call. All we would hear is a buzz. Several basic sine waves are combined to form a composite signal. A composite signal's bandwidth is the set of frequencies it contains. In most cases, the bandwidth simply the difference between two numbers. A composite signal's bandwidth, for instance, is 5000 – 1000, or 4000, if its frequencies range from 1000 to 5000. The difference between the highest and lowest frequencies included in a composite signal is known as its bandwidth[11]. The periodic signal's bandwidth includes all integer frequencies between 1000 and 5000. (1000, 100 I, 1002,). The no periodic signals have a similar bandwidth, but their frequencies are continuous.

CONCLUSION

Data and signals are two fundamental concepts in modern communication and information technology. While they are distinct concepts, they are closely related and are essential to the transmission, processing, and analysis of information. The transmission of signals is subject to various forms of noise and interference, which can be mitigated using various techniques, such as error-correcting codes, signal processing algorithms, and modulation techniques. Data and signals are used in various applications, such as telecommunications, computing, media, healthcare, and finance, and are key enablers of innovation and progress in the digital age.

REFERENCES

[1] B. Rim, N. J. Sung, S. Min, and M. Hong, "Deep learning in physiological signal data: A survey," *Sensors (Switzerland)*. 2020. doi: 10.3390/s20040969.

[2] Y. K. Wan, C. Hendra, P. N. Pratanwanich, and J. Göke, "Beyond sequencing: machine learning algorithms extract biology hidden in Nanopore signal data," *Trends in Genetics*. 2022. doi: 10.1016/j.tig.2021.09.001.

[3] A. L. Washington, "Uncertain risk: assessing open data signals," *Transform. Gov. People, Process Policy*, 2020, doi: 10.1108/TG-09-2019-0086.

[4] C. Orphanidou, "A review of big data applications of physiological signal data," *Biophysical Reviews*. 2019. doi: 10.1007/s12551-018-0495-3.

[5] J. M. Ferguson and M. A. Smith, "SquiggleKit: A toolkit for manipulating nanopore signal data," *Bioinformatics*, 2019, doi: 10.1093/bioinformatics/btz586.

[6] H. F. Posada-Quintero and K. H. Chon, "Innovations in electrodermal activity data collection and signal processing: A systematic review," *Sensors (Switzerland)*. 2020. doi: 10.3390/s20020479.

[7] P. Dai, S. Zhang, Y. Gong, Y. Zhou, and H. Hou, "A crowd-sourced valuation of recreational ecosystem services using mobile signal data applied to a restored wetland in China," *Ecol. Econ.*, 2022, doi: 10.1016/j.ecolecon.2021.107249.

[8] S. S. Sahoo *et al.*, "NeuroPigPen: A scalable toolkit for processing electrophysiological signal data in neuroscience applications using apache pig," *Front. Neuroinform.*, 2016, doi: 10.3389/fninf.2016.00018.

[9] K. M. Aquino, B. D. Fulcher, L. Parkes, K. Sabaroedin, and A. Fornito, "Identifying and removing widespread signal deflections from fMRI data: Rethinking the global signal regression problem," *Neuroimage*, 2020, doi: 10.1016/j.neuroimage.2020.116614.

[10] E. Stassen *et al.*, "Ultra-low power all-optical wavelength conversion of high-speed data signals in high-confinement AlGaAs-on-insulator microresonators," *APL Photonics*, 2019, doi: 10.1063/1.5115232.

[11] C. Jayapandian *et al.*, "A scalable neuroinformatics data flow for electrophysiological signals using MapReduce," *Front. Neuroinform.*, 2015, doi: 10.3389/fninf.2015.00004.

CHAPTER 7

DIGITAL TRANSMISSION: A COMPARATIVE STUDY ON MODULATION TECHNIQUES AND CHANNEL CODING FOR RELIABLE AND EFFICIENT COMMUNICATION

Dr. Abhishek Kumar Sharma, Assistant Professor,
Department of Computer Science, Sanskriti University, Mathura, Uttar Pradesh, India,
Email id- abhishek.sharma@sanskriti.edu.in

ABSTRACT:

Digital transmission refers to the process of sending digital data over a communication channel from one location to another. This type of transmission is widely used in modern telecommunications, including internet communication, wireless networks, and mobile communication. Digital transmission is achieved through a series of processes that convert analog signals into digital signals for transmission. This includes sampling, quantization, and encoding of the analog signal into a digital signal that can be easily transmitted and decoded at the receiving end.

KEYWORDS:

Analog Signal, Digital Transmission, Digital Signals, Internet Communication, Wireless Network.

INTRODUCTION

Digital signals are less prone to noise and interference, which can degrade the quality of the transmitted data. Additionally, digital transmission allows for the use of advanced error correction techniques, which further enhances the reliability of the communication [1]–[3] . There are several methods for digital transmission, including baseband transmission, broadband transmission, and carrier modulation techniques such as amplitude, frequency, and phase modulation. Each method has its own advantages and disadvantages, depending on the application. There are several key concepts in digital transmission that are essential to understanding the technology. These include:

1. **Digital Signals:** A digital signal is a binary sequence of 1s and 0s that represent the data being transmitted. These signals can be transmitted over a communication channel in a variety of ways, including through wires, optical fibers, or wireless networks.
2. **Sampling:** Sampling is the process of measuring the amplitude of a continuous signal at regular intervals. This converts an analog signal into a digital signal, which can then be processed by a computer or other digital device.
3. **Quantization:** Quantization is the process of mapping the continuous amplitude of an analog signal to a finite number of discrete levels. This allows the analog signal to be represented by a series of binary digits (bits) that can be transmitted over a communication channel.

4. **Encoding:** Encoding is the process of converting the binary sequence of 1s and 0s into a digital signal that can be transmitted over a communication channel. This can be done using various encoding techniques, such as pulse amplitude modulation (PAM), pulse code modulation (PCM), or quadrature amplitude modulation (QAM).

Methods of Digital Transmission

There are several methods of digital transmission, each with its own advantages and disadvantages. The three primary methods are baseband transmission, broadband transmission, and carrier modulation techniques.

1. **Baseband Transmission:** In baseband transmission, digital signals are transmitted directly over a communication channel without any modulation. This method is typically used for short-distance communication, such as within a building or a local area network (LAN).
2. **Broadband Transmission:**Broadband transmission involves the use of multiple channels to transmit digital signals simultaneously. This method is typically used for long-distance communication, such as over a wide area network (WAN) or the internet.
3. **Carrier Modulation Techniques:** Carrier modulation techniques involve the use of a carrier signal to transmit digital data. The most common carrier modulation techniques are amplitude modulation (AM), frequency modulation (FM), and phase modulation (PM).

Amplitude Modulation (AM)

In amplitude modulation, the amplitude of a carrier signal is modulated by the digital signal to be transmitted. This results in a signal with varying amplitude, which can be decoded at the receiving end to extract the original digital signal. AM is commonly used for radio and television broadcasting.

Frequency Modulation (FM)

In frequency modulation, the frequency of a carrier signal is modulated by the digital signal to be transmitted. This results in a signal with varying frequency, which can be decoded at the receiving end to extract the original digital signal. FM is commonly used for FM radio broadcasting and some wireless communication systems.

Phase Modulation (PM)

In phase modulation, the phase of a carrier signal is modulated by the digital signal to be transmitted. This results in a signal with varying phase, which can be decoded at the receiving end to extract the original digital signal. PM is commonly used for satellite communication systems and some digital cellular networks.

Error Correction Techniques

One of the most significant advantages of digital transmission over analog transmission is the ability to use error correction techniques to enhance the reliability of the communication process. Error correction techniques can detect and correct errors in the transmitted data, ensuring that the data is received accurately and without corruption.There are several error correction techniques, including forward error correction (FEC)

Forward Error Correction (FEC)

Forward error correction (FEC) is a technique that adds redundant information to the transmitted data, allowing errors to be detected and corrected at the receiving end. This is achieved by adding extra bits to the original data, which are used to verify the accuracy of the transmitted data. If an error is detected, the redundant information can be used to correct the error and restore the original data. FEC is commonly used in digital communication systems, including satellite communication, digital television, and wireless networks. The amount of redundancy added to the data is determined by the required level of error correction and the available bandwidth.

Automatic Repeat Request (ARQ)

Automatic repeat request (ARQ) is a technique that involves the sender resending data if errors are detected at the receiving end. In ARQ, the receiver sends an acknowledgement (ACK) or negative acknowledgement (NACK) to the sender, indicating whether the transmitted data was received correctly or not. If a NACK is received, the sender resends the data until an ACK is received. ARQ is commonly used in digital communication systems, including wireless networks and the internet. The number of times the data is resent is determined by the level of error correction required and the available bandwidth [4].

Cyclic Redundancy Check (CRC)

Cyclic redundancy check (CRC) is a technique that involves adding a checksum to the transmitted data, allowing errors to be detected at the receiving end. This is achieved by dividing the data by a predefined polynomial and adding the remainder as a checksum to the transmitted data. At the receiving end, the data is divided by the same polynomial, and the remainder is compared to the received checksum. If the two values do not match, an error is detected.

CRC is commonly used in digital communication systems, including Ethernet networks, digital television, and wireless networks. Digital transmission has revolutionized the field of telecommunications, enabling faster, more reliable, and efficient communication over long distances. Digital transmission is achieved through a series of processes that convert analog signals into digital signals for transmission. The primary advantage of digital transmission is that it is more reliable and efficient than analog transmission. Digital signals are less prone to noise and interference, which can degrade the quality of the transmitted data. Additionally, digital transmission allows for the use of advanced error correction techniques, which further enhances the reliability of the communication [5], [6].

There are several methods for digital transmission, including baseband transmission, broadband transmission, and carrier modulation techniques such as amplitude, frequency, and phase modulation. Each method has its own advantages and disadvantages, depending on the application. Overall, digital transmission is an essential technology that enables the modern world of telecommunications, powering communication over the internet, wireless networks, and mobile communication. With the continued development of digital transmission technology, we can expect even faster, more reliable, and efficient communication in the years to come.

DISCUSSION

Digital transmission refers to the process of transmitting data in a digital format from one location to another. The data is encoded into a series of bits, which are then transmitted over a

communications channel, such as a wire, cable, or radio waves. The digital transmission is widely used in modern communication systems, including telephone networks, computer networks, and satellite communication systems. The basic process of digital transmission involves three key stages: encoding, modulation, and transmission. In the encoding stage, the data is transformed into a sequence of bits, which can be represented using a binary code. For example, in a computer network, digital data is encoded using the ASCII code, which assigns a unique binary code to each character [7], [8].

In the modulation stage, the digital signal is modulated onto a carrier wave, which is a continuous sine wave with a specific frequency and amplitude. The process of modulation involves changing the frequency, phase, or amplitude of the carrier wave in response to the digital signal. There are several types of modulation techniques, including amplitude modulation (AM), frequency modulation (FM), phase modulation (PM), and quadrature amplitude modulation (QAM). Once the signal has been modulated, it can be transmitted over a communications channel, which can be wired or wireless. In a wired channel, the signal is transmitted over a physical cable, such as a coaxial cable or fiber optic cable. In a wireless channel, the signal is transmitted over the airwaves, using radio waves or microwaves.

The process of digital transmission is subject to various types of noise and distortion, which can affect the quality of the transmitted signal. Some of the common types of noise include thermal noise, intermodulation noise, and cross-talk. To minimize the effect of noise, various techniques are used, such as error correction codes, signal processing, and equalization. One of the key advantages of digital transmission over analog transmission is its ability to transmit data over longer distances without degradation of the signal. Digital signals can be amplified and regenerated, without losing any information, which makes them more resilient to noise and distortion. In addition, digital transmission is more versatile than analog transmission, as it can support a wide range of data types, including text, images, video, and audio.

Another advantage of digital transmission is its ability to multiplex multiple signals onto a single communications channel. Multiplexing refers to the process of combining multiple signals into a single signal, which can be transmitted over a shared medium [9] . Multiplexing can be achieved in several ways, including time-division multiplexing (TDM), frequency-division multiplexing (FDM), and code-division multiplexing (CDM). In time-division multiplexing, the signals are transmitted in discrete time slots, which are allocated to different signals. Each signal is transmitted in its allocated time slot, and the signals are interleaved to form a single signal. In frequency-division multiplexing, the signals are transmitted at different frequencies, which are separated by a guard band. Each signal occupies a specific frequency band, and the signals are combined to form a single signal. In code-division multiplexing, the signals are transmitted using different codes, which are combined to form a single signal.

Digital transmission is used in various types of communication systems, including telephone networks, computer networks, and satellite communication systems. In a telephone network, digital transmission is used to carry voice calls over a network of switches and transmission lines. The voice signals are digitized and compressed, and then transmitted over the network using a time-division multiplexing technique. In a computer network, digital transmission is used to transmit data between computers and other devices. The data is encoded using a variety of protocols, such as Ethernet, TCP/IP, and Wi-Fi. The digital signals are transmitted over a wired

or wireless medium, using various modulation techniques, such as amplitude modulation, frequency modulation, or phase modulation.

Satellite communication systems use digital transmission to transmit data over long distances, including television broadcasts, weather information, and GPS signals. The data is transmitted to and from satellites in space, using various modulation techniques and multiplexing methods.

Digital transmission is also used in various other applications, such as digital television, digital audio, and digital photography. Digital television uses digital transmission to deliver high-quality television signals, which can be transmitted over the airwaves or through cable or satellite networks. Digital audio uses digital transmission to store and transmit high-quality audio signals, which can be stored on CDs, MP3 players, or streamed over the internet [10]. Digital photography uses digital transmission to store and transmit high-resolution images, which can be stored on memory cards, transmitted over Wi-Fi, or uploaded to cloud storage services.

The quality of digital transmission can be measured using various metrics, such as signal-to-noise ratio, bit error rate, and throughput. Signal-to-noise ratio (SNR) is a measure of the strength of the signal compared to the level of background noise. A higher SNR indicates a better quality signal. Bit error rate (BER) is a measure of the number of bit errors that occur during transmission. A lower BER indicates a better quality signal. Throughput is a measure of the amount of data that can be transmitted over a communications channel, usually expressed in bits per second (bps).

To improve the quality of digital transmission, various techniques are used, such as error correction codes, signal processing, and equalization. Error correction codes are used to detect and correct errors that occur during transmission, using algorithms such as Reed-Solomon codes, convolutional codes, or turbo codes. Signal processing techniques are used to enhance the quality of the signal, by removing noise, distortion, or interference. Equalization techniques are used to compensate for the effects of attenuation and distortion on the signal, by adjusting the amplitude and phase of the signal.

The purpose of a computer network is to transfer data from one location to another. For transmission, this data has to be transformed into either a digital signal or an analogue signal. The first option, conversion to digital signals, is covered in this chapter; the second option, conversion to analogue signals. We covered the benefits and drawbacks of digital transmission over analogue transmission. We demonstrate the strategies and methods for digital data transmission in this chapter. We begin by talking about ways for converting digital data to digital signals, or digital-to-digital conversion. In the next section, we go through approaches for converting analogue signals into digital signals. We talk about transmission modes last.

Data may either be digital or analogue, as we previously said. We also said that data transmissions might be either digital or analogue. This section demonstrates how digital signals may be used to represent digital data. Line coding, block coding, and scrambling are the three strategies used during the conversion. Block coding, scrambling mayor, and line coding are never unnecessary. Digital data is transformed into digital signals via the process of line coding. We presume that data is stored in computer memory as a series of bits, whether it be text, numbers, visual pictures, audio, or video. A series of bits is transformed into a digital signal via line coding. Digital data are encoded into a digital signal at the transmitter, and the digital signal is decoded at the receiver to reproduce the digital data.

Comparison of the Signal and Data Elements Let's tell the difference between a signal element and a data element. Our objective in data communications is to communicate data components. The smallest unit that may represent a piece of information is called a data element, or bit. A signal element carries data components in digital data transfers. The smallest (temporally) component of a digital signal is known as a signal element. In other words, we may convey signal elements but just need to provide data items. Signal elements serve as the carriers and carry data components.

Signal versus data rate the quantity of data elements (bits) delivered in Is is determined by the data rate. It measures bits per second (bps). The quantity of signal components conveyed in IS is known as the signal rate. The baud is the unit. The literature uses a number of standard terms. Although the signal rate is sometimes referred to as the pulse rate, modulation rate, or baud rate, the data rate is often referred to as the bit rate. Increasing the data rate while lowering the signal rate is one objective in data communications. The speed of transmission is increased by increasing the data rate, while the bandwidth need is decreased by reducing the signal rate. To avoid traffic congestion, in our vehicle-people analogy, we must transport more people in fewer cars. The available bandwidth in our transportation system is limited.

The link between data rate and signal rate (bit rate and baud rate) must now be taken into account. Of course, the value of r has an impact on this connection. The data pattern is another factor. The signal rate may change from a data pattern with alternating Os and is if we have a data pattern with all 1s or all Os. We need to specify three cases: the worst, best, and average in order to create a formula for the connection. The worst case scenario is when we need the highest signal rate, and the ideal scenario is when we require the lowest. In data communications, the typical instance is what most interests us. The link between data rate and signal rate may be expressed as 1 N is the data rate (bps); c is the case factor, which changes for each case; S is the number of signal elements; and r is the previously specified factor. One data element is represented as one signal element in a signal conveying data (r = 1). What is the average baud rate if c is between 0 and l and the bit rate is 100 kbps?

Assumedly, c has an average value of. Hence, S =c x N x - 111 = - x 100,000 x -1 = 50,000 =50 kbaud r 2 Bandwidth is the baud rate. A digital signal that conveys information is no periodic, as was mentioned. We also demonstrated that a no periodic signal's bandwidth is continuous and has an indefinite range bandwidth with finite values, on the other hand, characterizes the majority of digital signals we come across in daily life. In other words, even if the bandwidth is theoretically limitless, many of the components are too tiny to be seen. The actual bandwidth has a limit. From now on, we must keep in mind that we are referring to this effective bandwidth whenever we discuss the bandwidth of a digital transmission.

The effective bandwidth of a digital transmission is unlimited, despite the fact that the real bandwidth is limitless. We may state that the needed bandwidth for a digital transmission is determined by the baud rate rather than the bit rate. If we compare traffic to transportation, the number of cars, not the number of persons being transported, determines the flow of traffic. Additional signal modifications include adding more frequencies to the signal. Remember that change equals frequency and frequency equals change. The required frequency range is reflected in the bandwidth.

There is a connection between the bandwidth and the baud rate (signal rate). An intricate concept, bandwidth. Usually, when we discuss bandwidth, we refer to a range of frequencies.

The locations of this range and the frequencies' lowest and greatest values are both important to know. Also, each component's amplitude (if not its phase) is a crucial consideration. In other words, we need a bandwidth diagram in addition to merely knowing the value of the bandwidth. For the majority of the schemes covered in this chapter, we shall display the bandwidth. Right now, we can state that the bandwidth (spectrum of frequencies) is inversely correlated with the signal rate (baud rate). The formula for the minimal bandwidth is 1 Bmin = c > N > - r.

If we know the channel's bandwidth, we can find the maximum data rate xBxr = 1 Nmax Many strategies have been developed in an effort to boost data speed or minimize bandwidth requirements. By converting a pattern of m data elements into a pattern of n signal elements, it is possible to increase the number of bits per baud. As there are only two kinds of data components in use (Os and Is), a collection of m data items may combine to form any one of m data patterns. By allowing for various signal levels, we may have several signal element kinds. We can create Ln various signal pattern combinations if we have L different levels. Each data pattern is converted into one signal pattern if 2m = Ln. Data patterns only make up a portion of signal patterns if 2m Ln. The subset may be carefully planned to avoid baseline wandering, to provide synchronization, and to identify transmission faults. If 2m > Ln, data encoding is impossible because certain data patterns cannot be encoded.

The length of the binary pattern, the amount of binary data, the length of the signal pattern, and the number of levels in the signaling are all indicated by the letters m, B, n, and L, respectively, in the classification of various sorts of coding by code designers. L is often replaced by a letter, such as B for L = 2, T for L = 3, and Q for L = 4. The data pattern is defined by the first two letters, while the signal pattern is defined by the second two. A pattern of m data elements in mBnL schemes is represented as a pattern of n signal elements where 2m; Ln the first mBnL system we cover, 2BIQ (two binary, one quaternary), employs 2-bit data patterns and encodes them as one signal element of a 4-level signal. This method of encoding uses m = 2, n = 1, and L = 4. (quatemary).

2BlQ's typical signal rate is S = N/4. This indicates that employing 2BIQ will enable us to deliver data twice as quickly as NRZ-L. The receiver must be able to distinguish four distinct thresholds since 2B lQ employs four different signal levels. Costs are associated with the decreased bandwidth. This method has no duplicate signal patterns since 22 = 41. BIQ is a component of DSL (Digital Subscriber Line) technology, which uses subscriber telephone lines to provide a high-speed access to the Internet. The eight binary, six ternary arrangement is really intriguing (8B6T). We shall see how to utilise this code with 100BASE-4T cable. An 8-bit pattern is intended to be encoded as a pattern of six signal components, where the signal has three levels (ternary). We can have 28 = 256 distinct data patterns and 36 = 478 various signal patterns in this kind of approach. In Appendix D, the mapping table is shown. The redundant signal components for synchronisation and error detection are 478 - 256 = 222. DC balancing is also achieved in part via redundancy. The weight of each signal pattern is either 0 or +1 DC values. This indicates that the weight -1 has no pattern. The transmitter monitors the weight to maintain the whole stream Dc-balanced. When two successive groups of weight 1 are met, the first one is delivered just as it is, while the second one is completely inverted to produce a weight of -1.

An example of three data patterns being encoded as three signal patterns. The three different signal levels are denoted by the symbols -, 0 and +. The signal pattern -0-0++ with weight 0 is

used to encode the first 8-bit pattern, 00010001, whereas the signal pattern - + - + + + 0 with weight +1 is used to encode the second 8-bit pattern, 010 10011. It is recommended to encode the third bit pattern as + - - + 0 + with weight +1. The transmitter inverts the original signal to provide DC balance. Since the weight is -1, the receiver can immediately see that this is an inverted pattern. Decoding begins by inverting the pattern. Theoretically, the scheme's average signal rate is Save =! X N X; in actuality, the minimum bandwidth is extremely near 6N18. 2 8 4D-PAMS This category's final signalling method is known as four-dimensional five-level pulse amplitude modulation (4D-PAM5). The 4D abbreviation denotes simultaneous data transmission across four lines. Five voltage levels are used, including -2, -1, 0, 1, and 2.

Level 0, however, is the sole level that is used for forward error detection (discussed in Chapter 10). The four layers produce something that resembles 8B4Q if we believe that the code is just one dimension. In other words, a signal element with four levels is created from an 8-bit word. For this hypothetical one-dimensional variant, the worst signal rate is N X 4/8, or N12. The method is intended to deliver data over four channels (four wires). As a result, the signal rate may be lowered to N18, which is an important accomplishment. One signal element may be used to transmit all 8 bits concurrently onto a wire. The key here is that a signal group's four signal parts are conveyed concurrently in a four-dimensional environment. The hypothetical one-dimensional and the real four-dimensional implementations.

This method is used by Gigabit LANs to transmit 1-Gbps data via four copper wires that can process 125 Mbaud. Due to the fact that 28 data patterns are matched to 44 = 256 signal patterns in this technique, there is a lot of signal pattern redundancy. Further uses, such as error detection, may be made of the additional signal patterns. One could question the need of MLT-3, a mapping mechanism from one bit to one signal element. While more complicated, the signal rate is the same as for NRZ-I. (Three levels and complex transition rules). It turns out that the signal's structure in this technique aids in lowering the necessary bandwidth. Let's examine the worst-case situation, which is sequence. The signal element pattern in this instance is +VO - VO, which is repeated every 4 bits.

With a period equal to four times the bit duration, a no periodic signal has become periodic. One may mimic the worst-case scenario as an analogue signal with a frequency equal to one-fourth of the data rate. In other words, MLT-3's signal rate is one-fourth that of its bit rate. As a result, MLT-3 is a good option if you need to transport 100 Mbps across a copper cable that can only handle 32 MHz of frequency anything more results in electromagnetic emissions. Redundancy is necessary to maintain synchronization and to provide some kind of built-in error detection. This redundancy may be provided using block coding, which also enhances line coding's performance. Block coding, in general, converts an initial block of m bits into an initial block of n bits, where n is more than m. An mB/nB encoding approach is what block coding is known as.

Block encoding is distinguished from multilayer encoding, which is expressed without a slash, by the use of a slash (for example, 4B/5B). The three processes of block coding are typically division, substitution, and combination. A sequence of bits is separated into groups of m bits in the division step. For instance, the original bit sequence is broken into 4-bit groups in 4B/5B encoding. The replacement stage is the core of block coding. At this stage, an m-bit group is used in place of an n-bit group.

For instance, in 4B/5B encoding, a 4-bit code is used in place of a 5-bit group. The n-bit groups are then merged to create a stream. More bits than the original bits are in the new stream. The

process. In order to work with NRZ-I, the four binary/five binary (4B/5B) coding scheme was created. As you may recall, NRZ-I has an excellent signal rate about half that of biphasicbut synchronization issues. The receiver clock may get out of sync if there is a prolonged series of as. One approach is to modify the bit stream such that it doesn't contain a lengthy stream of as before encoding with NRZ-I. The 4B/5B scheme succeeds in this endeavor. As we shall see later, the block-coded stream does not include more than three consecutive as. The NRZ-I encoded digital signal is first decoded at the receiver into a stream of bits, and then the redundant information is removed. In 4B/5B, there can only be one leading zero (left bit) and a maximum of two following zeros in the 5-bit output that substitutes the 4-bit input (right bits). There are thus never more than three consecutive as when various groups are merged to create a new sequence.

(Notice that NRZ-I has no issues with isolating sequences.) The equivalent pairings used in 4B/5B encoding. The first two columns, it should be noted, couple a 4-bit group with a 5-bit group. A group of 4 bits can only be combined in 16 distinct ways, but a group of 5 bits may be combined in 32 different ways. This indicates that 16 groups are available for 4B/5B encoding but are not utilized. Some of these underutilized groups are used for control, while others are never used. They provide a kind of error detection. The receiver is alerted to a transmission problem if a 5-bit group that corresponds to the table's unused region is received. Similar to the 4B/5B encoding, the eight binary/ten binary (SBIlOB) encoding substitutes a group of 8 bits of data with a lO-bit code. Compared to 4B/5B, it has better mistake detection capabilities.

A 10 bit block's five most significant bits are sent into a 5B/6B encoder, while its three least important bits are put into a 3B/4B encoder. To make the mapping table simpler, a split was performed. The code employs a disparity controller, which keeps track of excess Os over Is, to avoid extended runs of consecutive Os or Is (or Is over Os). Each bit in the code is complemented if the gap between the bits in the current block and the bits in the preceding block increases (in either direction) (a 0 is changed to a 1 and a 1 is changed to a 0).

The redundant groups in the code, which have a total of 210 - 28 = 768, may be utilised to check for disparities and spot errors. The approach has greater built-in error-checking and better synchronisation than 4B/5B, making it generally preferable.

Scrambling Biphase systems with their high bandwidth requirements are more suited for dedicated lines between stations in a LAN than they are for long-distance communication. Because of the DC component, block coding and NRZ line coding are also not appropriate for long-distance encoding. Contrarily, bipolar AMI encoding has a small bandwidth and doesn't produce a DC component. A lengthy process, however, throws off the synchronization. We can employ bipolar AMI over long distances if we can figure out a means to prevent a lengthy series in the original stream.

We are searching for a method that provides synchronization while without adding more bits. In order to achieve synchronization, we are searching for a solution that swaps out lengthy zero-level pulses for a mix of different levels. Scrambling is one approach. We change a portion of the AMI rule to incorporate scrambling. It should be noted that scrambling as opposed to block coding takes place concurrently with encoding. Based on the specified scrambling rules, the system must inject the necessary pulses. The B8ZS and HDB3 scrambling methods are two popular ones. In North America, R8ZS Bipolar with S-zero Substitution (BSZS) is widely utilized. This method replaces eight consecutive zero-level voltages with the sequence

CONCLUSION

Digital transmission is a fundamental process in modern communication systems, which involves encoding data into a series of bits, modulating the digital signal onto a carrier wave, and transmitting the signal over a communications channel [11]. Digital transmission has several advantages over analog transmission, including greater resilience to noise and distortion, greater versatility in supporting different types of data, and the ability to multiplex multiple signals onto a single communications channel. Digital transmission is used in various types of communication systems, including telephone networks, computer networks, and satellite communication systems. To improve the quality of digital transmission, various techniques are used, such as error correction codes, signal processing, and equalization.

REFERENCES

[1] T. Kang, K. Il Oh, H. Park, and S. Kang, "Review of capacitive coupling human body communications based on digital transmission," *ICT Express*. 2016. doi: 10.1016/j.icte.2016.11.002.

[2] G. Xin and Z. Jinbao, "An APD-based evaluation on the effect of transient disturbance over digital transmission," *Chinese J. Electron.*, 2020, doi: 10.1049/cje.2019.09.007.

[3] M. M. Amiri, D. Gunduz, S. R. Kulkarni, and H. V. Poor, "Convergence of Federated Learning over a Noisy Downlink," *IEEE Trans. Wirel. Commun.*, 2022, doi: 10.1109/TWC.2021.3103874.

[4] M. Zbili and D. Debanne, "Past and future of analog-digital modulation of synaptic transmission," *Frontiers in Cellular Neuroscience*. 2019. doi: 10.3389/fncel.2019.00160.

[5] B. Bossy, P. Kryszkiewicz, and H. Bogucka, "Flexible, brain-inspired communication in massive wireless networks," *Sensors (Switzerland)*, 2020, doi: 10.3390/s20061587.

[6] R. Malikov, "DIGITAL TRANSMISSION SYSTEM," *EurasianUnionScientists*, 2021, doi: 10.31618/esu.2413-9335.2021.1.92.1508.

[7] X. Wan *et al.*, "User Tracking and Wireless Digital Transmission through a Programmable Metasurface," *Adv. Mater. Technol.*, 2021, doi: 10.1002/admt.202001254.

[8] C. H. Hyoung, S. W. Kang, S. O. Park, and Y. T. Kim, "Transceiver for human body communication using frequency selective digital transmission," *ETRI J.*, 2012, doi: 10.4218/etrij.12.0111.0178.

[9] S. Mangel, L. Gleim, J. Pennekamp, K. Wehrle, and S. Decker, "Data Reliability and Trustworthiness Through Digital Transmission Contracts," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2021. doi: 10.1007/978-3-030-77385-4_16.

[10] M. Teixeira and V. Zaharov, "Digital Transmission," in *Handbook of Computer Networks*, 2011. doi: 10.1002/9781118256053.ch7.

[11] P. Bergadà *et al.*, "Digital transmission techniques for a long haul HF link: DSSS versus OFDM," *Radio Sci.*, 2014, doi: 10.1002/2013RS005203.

CHAPTER 8

SIGNAL ENCODING TECHNIQUES: A COMPREHENSIVE ANALYSIS OF ENCODING SCHEMES FOR EFFICIENT AND SECURE DIGITAL COMMUNICATION

Dr. Govind Singh, Assistant Professor,
Department of Computer Science, Sanskriti University, Mathura, Uttar Pradesh, India,
Email id- govind@sanskriti.edu.in

ABSTRACT:

Signal encoding techniques are fundamental to digital communication systems. These techniques involve the process of converting analog signals into digital signals, which can be transmitted over a communications channel. This abstract will provide an overview of the different types of signal encoding techniques, including pulse code modulation (PCM), delta modulation, and adaptive delta modulation. PCM is the most common signal encoding technique, and involves the quantization of an analog signal into a series of digital values. The process involves sampling the analog signal at regular intervals, and then assigning each sample a digital value based on its amplitude. The digital values are then transmitted over the communications channel, and can be reconstructed into an analog signal at the receiver. PCM is a robust technique that provides good signal-to-noise ratio and dynamic range, but it can be bandwidth-intensive due to the large number of bits required for each sample.

KEYWORDS:

Analog Signals, Bandwidth, Digital Communication, Digital Signals, Pulse Code.

INTRODUCTION

Signal encoding techniques are the methods used to convert analog signals into digital form for effective transmission, storage, and processing. Analog signals are continuous and are used to convey information in the form of electric voltage, current, or frequency variations. In contrast, digital signals are discrete and are represented using binary code, which comprises of a combination of 0s and 1s. The digital signals are easy to transmit and process since they are less susceptible to noise and distortion compared to analog signals [1]–[3] . This article provides an in-depth overview of the signal encoding techniques used to convert analog signals into digital form.

1. **Pulse Code Modulation (PCM):** Pulse code modulation (PCM) is a technique used to digitize analog signals. In PCM, the analog signal is sampled at a regular interval, and each sample is quantized into a digital code. The sampling rate determines the accuracy of the reconstructed signal. The higher the sampling rate, the more accurate the reconstructed signal. PCM is widely used in digital audio and video systems, digital telephony, and data communication systems.
2. **Differential Pulse Code Modulation (DPCM):** Differential pulse code modulation (DPCM) is a modification of PCM, where instead of quantizing the sample directly, the difference between the sample and the predicted sample value is quantized. The predicted sample value is the previously quantized sample value. DPCM reduces the number of bits

required to represent the sample by exploiting the correlation between the adjacent samples. DPCM is used in speech and image compression.

3. **Delta Modulation (DM):** Delta modulation (DM) is a simplified version of DPCM, where instead of quantizing the difference between the sample and the predicted sample value, the difference is approximated using a one-bit quantizer. Delta modulation is a low-complexity method for digitizing analog signals but is highly sensitive to noise and distortion.
4. **Adaptive Delta Modulation (ADM):** Adaptive delta modulation (ADM) is an improvement over delta modulation, where the step size of the quantizer is adjusted based on the level of the input signal. The step size is increased if the input signal level is high and decreased if the input signal level is low. ADM provides a better trade-off between complexity and performance than DM.
5. **Pulse Width Modulation (PWM):** Pulse width modulation (PWM) is a technique used to encode analog signals in a digital form by varying the width of the pulse. The width of the pulse represents the amplitude of the analog signal. The pulse is usually a square wave with a fixed frequency. PWM is widely used in motor control, power electronics, and audio systems.
6. **Pulse Position Modulation (PPM):** Pulse position modulation (PPM) is a technique used to encode analog signals in a digital form by varying the position of the pulse. The position of the pulse within the fixed interval represents the amplitude of the analog signal. PPM is less susceptible to noise and distortion compared to PWM, but it requires a higher bandwidth.
7. **Frequency Shift Keying (FSK):** Frequency shift keying (FSK) is a technique used to encode analog signals in a digital form by varying the frequency of the carrier wave. The frequency of the carrier wave is shifted between two values to represent the binary code. FSK is widely used in radio frequency communication systems.
8. **Phase Shift Keying (PSK):** Phase shift keying (PSK) is a technique used to encode analog signals in a digital form by varying the phase of the carrier wave. The phase of the carrier wave is shifted between two or more values to represent the binary code. PSK is widely used in digital communication systems and satellite communication.
9. **Amplitude Shift Keying (ASK):** Amplitude shift keying (ASK) is a technique used to encode analog signals in a digital form by varying the amplitude of the carrier wave. The amplitude of the carrier wave is changed between two or more values to represent the binary code. ASK is a simple and low-cost modulation technique used in digital communication systems, but it is less immune to noise and distortion compared to other modulation techniques.
10. **Quadrature Amplitude Modulation (QAM):** Quadrature amplitude modulation (QAM) is a modulation technique that combines amplitude and phase modulation to increase the data rate of digital communication systems. QAM uses two carriers that are out of phase with each other and modulates them with two different binary codes. The amplitude and phase of the carrier waves are changed to represent the binary codes. QAM is widely used in digital television, cable modems, and wireless communication systems.

11. **Time Division Multiplexing (TDM):** Time division multiplexing (TDM) is a technique used to transmit multiple signals over a single transmission medium. TDM divides the time into multiple time slots, and each signal is transmitted in a separate time slot. TDM is used in digital telephony, where multiple voice channels are multiplexed over a single transmission line.
12. **Frequency Division Multiplexing (FDM):** Frequency division multiplexing (FDM) is a technique used to transmit multiple signals over a single transmission medium. FDM divides the frequency band into multiple frequency channels, and each signal is transmitted in a separate frequency channel. FDM is used in radio and television broadcasting, where multiple channels are multiplexed over a single transmission medium.
13. **Code Division Multiplexing (CDM):** Code division multiplexing (CDM) is a technique used to transmit multiple signals over a single transmission medium using code sequences. CDM assigns a unique code sequence to each signal, and all signals are transmitted simultaneously over the same frequency band. CDM is widely used in wireless communication systems, such as CDMA (code division multiple access) and WCDMA (wideband code division multiple access).
14. **Spread Spectrum Modulation (SSM):** Spread spectrum modulation (SSM) is a modulation technique that spreads the signal over a wide frequency band to increase its immunity to noise and interference. SSM uses a code sequence to spread the signal, and the receiver uses the same code sequence to extract the original signal. SSM is widely used in wireless communication systems, such as GPS (global positioning system) and WLAN (wireless local area network).
15. **Orthogonal Frequency Division Multiplexing (OFDM):** Orthogonal frequency division multiplexing (OFDM) is a modulation technique used to increase the data rate of digital communication systems. OFDM divides the frequency band into multiple subcarriers, and each subcarrier is modulated with a different binary code. The subcarriers are orthogonal to each other, which reduces the interference between them. OFDM is widely used in digital television, digital radio, and wireless communication systems.

Signal encoding techniques are essential in converting analog signals into digital form for effective transmission, storage, and processing. The choice of the encoding technique depends on the application requirements, such as data rate, complexity, and immunity to noise and interference. The above-listed signal encoding techniques are widely used in various applications, and they continue to evolve to meet the demands of the emerging digital technologies.

DISCUSSION

Signal encoding is the process of transforming analog or digital data into a form that can be transmitted or stored. The goal of signal encoding is to reduce the amount of data that needs to be transmitted or stored while maintaining the integrity of the data [4], [5]. There are several signal encoding techniques, each with its advantages and disadvantages. In this article, we will discuss various signal encoding techniques in detail.

In AM, the amplitude of the carrier signal is varied in proportion to the amplitude of the input signal. This results in a modulated signal that has a higher frequency than the input signal. The frequency of the carrier signal remains constant. AM is commonly used for broadcasting low-frequency signals, such as voice.

In FM, the frequency of the carrier signal is varied in proportion to the amplitude of the input signal. This results in a modulated signal that has a higher frequency than the input signal. The amplitude of the carrier signal remains constant. FM is commonly used for broadcasting high-frequency signals, such as music.

In PM, the phase of the carrier signal is varied in proportion to the amplitude of the input signal. This results in a modulated signal that has a higher frequency than the input signal. The frequency and amplitude of the carrier signal remain constant. PM is commonly used in digital communications. In PCM, an analog signal is sampled and converted into a digital signal. The amplitude of the analog signal is quantized into a fixed number of discrete values. PCM is commonly used for voice and music transmission.

In PAM, a digital signal is encoded as a sequence of pulses of varying amplitude. The amplitude of each pulse represents a binary value (0 or 1). PAM is commonly used in digital communications. PCM is also a digital signal encoding technique that was previously mentioned under analog signal encoding. In DPCM, the difference between two consecutive samples is quantized and transmitted instead of transmitting the actual sample value. DPCM is commonly used in image and video compression.

In DM, the difference between the input signal and a predicted value is quantized and transmitted. DM is commonly used for low-bandwidth transmission of speech and music. ADM is a variation of DM where the step size of the quantizer is adjusted based on the difference between the input signal and the predicted value. ADM is commonly used for low-bandwidth transmission of speech and music.

In DQPSK, the phase of the carrier signal is varied in four possible directions (0, $\pi/2$, π, $3\pi/2$) based on the value of the input signal. DQPSK is commonly used in digital communications. In QAM, the amplitude and phase of the carrier signal are varied based on the value of the input signal. QAM is commonly used in digital communications. In FSK, the frequency of the carrier signal is varied based on the value of the input signal. FSK is commonly used in digital communications.

In PSK, the phase of the carrier signal is varied based on the value of the input signal. PSK is commonly used in digital communications.In Manchester encoding, the data is encoded by changing the signal level in the middle of each bit. The signal transitions from low to high or high to low, in the middle of the bit interval, to represent a 1 or 0 respectively. Manchester encoding is commonly used in local area networks (LANs) such as Ethernet.

4B/5B encoding is a technique used to encode 4 bits of data into 5 bits of transmitted data. The encoding is necessary to ensure that a receiver can distinguish between valid and invalid data. 4B/5B encoding is used in various serial communication standards, including USB and Ethernet. 8B/10B encoding is similar to 4B/5B encoding but encodes 8 bits of data into 10 bits of transmitted data. 8B/10B encoding is used in various communication standards such as Fiber Channel and PCI Express.

RLE is a data compression technique that encodes consecutive data values as a count and a value pair. RLE is commonly used for image and video compression. Huffman encoding is a lossless data compression technique that assigns variable-length codes to symbols based on their frequency of occurrence. Huffman encoding is commonly used in image and video compression.

Arithmetic encoding is a lossless data compression technique that assigns variable-length codes to symbols based on their probability of occurrence. Arithmetic encoding is commonly used in image and video compression. LZW is a lossless data compression technique that encodes a string of symbols as a single code. LZW is commonly used in image and video compression. BWT is a reversible data compression technique that rearranges the input data to improve compressibility. BWT is commonly used in image and video compression.

Signal encoding is a crucial process in communication and data storage systems. Different encoding techniques are suitable for different applications and have their advantages and disadvantages. Analog signal encoding techniques such as AM, FM, PM, and PCM are commonly used for voice and music transmission. Digital signal encoding techniques such as PAM, PCM, DPCM, DM, ADM, DQPSK, QAM, FSK, PSK, Manchester encoding, 4B/5B encoding, 8B/10B encoding, RLE, Huffman encoding, arithmetic encoding, LZW, and BWT are commonly used in digital communications, image, and video compression, and data storage [6]. Understanding these signal encoding techniques is essential for designing efficient communication and data storage systems.

A data source g(t), which may be digital or analogue, is encoded into a digital signal x for use in digital signalling (t). The encoding method determines the precise shape of x(t), which is selected to make the most use of the transmission medium. For instance, the encoding may be selected to reduce mistakes or preserve bandwidth. A continuous, constant-frequency signal known as the carrier signal serves as the foundation for analogue communication. The carrier signal's frequency is selected to work with the specified transmission medium. By modulating a carrier signal, data may be transferred. Encoding source data with frequency on a carrier signal is called modulation. The three basic frequency domain characteristics of amplitude, frequency, and phase are used in all modulation schemes.

The modulating signal, also known as the baseband signal, is the input signal m(t), which may be either analogue or digital. The modulated signal is the outcome of modulating the carrier signal (t). S(t) is a signal that is band limited (bandpass). The bandwidth's position on the spectrum is connected to and often focuses on Once again, the actual encoding format is selected to improve a particular transmission feature. For each given communication goal, there are several justifications for selecting a certain combination.

Modulation is often used to move the bandwidth of a baseband signal to a different region of the spectrum. The A digital signal is composed of a series of discrete, discontinuous voltage pulses, each at a separate place. Each pulse is a component of a signal. Each data bit is converted into a signal element before being delivered as binary data. In the simplest scenario, bits and signal components are matched one to one.

We define a few words first. The signal is unipolar if each of the signal components has the same algebraic sign, that is, if they are all positive or all negative. In polar signaling, a positive voltage level represents one logic state, and a negative voltage level, the other. A signal's data signaling rate, or simply data rate, is the rate at which data are conveyed in bits per second.

A bit's duration, also known as its length, is the time it takes for the transmitter to emit it; given a data rate R, it is equal to 1/R. This will rely on the kind of digital encoding used, which is covered later. The baud unit, which stands for signal elements per second, is used to represent modulation rate. Lastly, for historical reasons, the names mark and space relate to the binary numbers 1 and 0, respectively [7], [8].

The tasks involved in deciphering digital signals at the receiver may be summed up. The receiver must first be aware of the time of each bit. That is, the beginning and end of a bit must be reasonably known by the receiver. Second, the receiver has to detect whether each bit position's signal level is high (0) or low (1) by sampling each bit location in the interval's center and comparing the result to a threshold. Errors will occur as a result of noise and other limitations, as shown. What elements influence the receiver's success in deciphering the incoming signal? Three elements, are significant: the range of signals: The signal spectrum has a number of crucial components. Less bandwidth is needed for transmission since there aren't as many high-frequency components present. Moreover, it is preferable to have no direct-current (dc) components. There must be a direct physical connection of transmission components when there is a dc component to the signal.

Transformer-based ac coupling is achievable without a dc component and offers great electrical isolation to minimized interference. Lastly, the spectral characteristics of the sent signal determine how much signal distortion and interference will affect the transmission. In actuality, it often occurs that a channel's transmission properties deteriorate towards the band margins. The transmitted power should thus be concentrated in the center of the transmission bandwidth in a suitable signal design. The received signal should exhibit less distortion in this scenario. Codes may be created with the intention of modifying the transmitted signal's spectrum in order to achieve this goal [9], [10].

We previously highlighted the need to establish the start and stop of each bit position. No simple job, this. Including a separate clock line to synchronize the transmitter and receiver is one fairly pricey solution. The alternative is to provide some kind of transmission-based synchronization method. This is possible with the right encoding, as will be discussed later. We'll go through a variety of error-detection methods and demonstrate that they fall within the purview of data link control, a level of logic that sits above the signaling level. Nonetheless, some error detection functionality that is included into the physical signals encoding technique is beneficial. This makes it possible to find faults more rapidly.In the presence of noise, certain codes function better than others. BERs are often used to describe performance. While the cost of digital logic is continuing to fall, this element should still be taken into consideration. In particular, the cost increases with the signaling rate needed to accomplish a given data throughput. We'll find that certain codes need signaling rates above and beyond the data rates in use.

Using two separate voltage levels for the two binary digits is the most typical and straightforward method of transmitting digital signals. The voltage level remains constant throughout a bit interval; there is no transition in the codes that use this method (no return to a zero voltage level). For instance, binary 0 may be represented by no voltage, whereas binary 1 can be represented by a steady positive voltage [11]. A negative voltage often corresponds to one binary value and a positive voltage to the other. Nonreturn to Zero-Level (NRZ-L) code, which is the latter. NRZ-L is often the code used by terminals and other devices to create or read digital

data. Whenever a different code has to be sent, the transmission system creates it from an NRZ-L signal NRZI is an alternative to NRZ (Nonreturn to Zero, invert on ones).

Similar to NRZ-L, NRZI maintains a steady voltage pulse throughout a bit period. The actual data are represented by the signal transition's existence or absence at the start of each bit period. If there is a transition (low to high or high to low) at the start of a bit time, that bit time is a binary 1; if there is none, it is a binary 0. A good example of differential encoding is NRZI. The information to be sent via differential encoding is expressed in terms of the differences between subsequent signal components rather than the actual signal elements. The following rules govern how the current bit is encoded: If the current bit is a binary 0, it is encoded with the same signal as the one that before it. If the current bit is a binary 1, a different signal from that which preceded it is used to encode it. The ability to identify a transition in the presence of noise more accurately than to compare a value to a threshold is one advantage of differential encoding.

Another advantage is that it is simple to lose track of the polarity of the signal when using a complicated transmission arrangement. For instance, all 1s and 0s for NRZ-L on a multidrop twisted-pair line will be reversed if the leads from a connected device to the twisted pair are unintentionally switched around. Differential encoding prevents this from happening. The NRZ codes use bandwidth well and are the simplest to design. The spectrum densities of several encoding techniques, provides an illustration of this latter characteristic. The frequency is normalized to the data rate in the graphic. Between dc and half the bit rate, NRZ and NRZI signals contain the majority of their energy. The majority of the energy in the signal is concentrated between dc and 4800 Hz, for instance, if an NRZ code is employed to create a signal with a data rate of 9600 bps.

The inclusion of a dc component and the absence of synchronization capabilities are the two fundamental drawbacks of NRZ transmissions. Consider that the output is a constant voltage over a lengthy period of time with a long string of 1s or 0s for NRZ-L or a long string of 0s for NRZI in order to visualize the latter issue. Under these conditions, any clock drift between the transmitter and receiver will cause the two to get out of sync. NRZ codes are often employed for digital magnetic recording due to their simplicity and very low frequency response properties. These codes are undesirable for signal transmission applications due to their drawbacks. Several of the NRZ codes' drawbacks are addressed by the multilevel binary encoding method category. These codes use a number of signal levels. A binary 1 is represented by a positive or negative pulse in the bipolar-AMI scheme whereas a binary 0 is represented by no line signal. The polarity of the binary 1 pulses must change. This strategy has a number of benefits.

First of all, if a lengthy string of 1s happens, synchronization will not be lost. The receiver may resynchronize on every 1 that introduces a transition. Even a lengthy run of 0s would provide a challenge. Second, there is no net dc component since the voltage of the 1 signals alternates between positive and negative. Moreover, the resultant signal's bandwidth is much less than the bandwidth for NRZ. Lastly, a straightforward method of error detection is offered by the pulse alternation feature. Each solitary mistake violates this condition, whether it adds or subtracts pulses. The remarks from the preceding sentence also apply to pseudo ternary. In this instance, the binary 0 is represented by alternating positive and negative pulses, while the binary 1 is symbolized by the lack of a line signal. Neither approach has a clear advantage over the other, yet both serve as the foundation for various applications.

While both codes provide some degree of synchronization, a lengthy series of 0s in the case of AMI or 1s in the case of pseudo ternary still poses a challenge. This shortcoming has been addressed using a variety of strategies. Inserting extra bits that cause transitions is one strategy. For somewhat slow data rate transfer, ISDN (integrated services digital network) uses this method. This method is obviously costly at large data rates since it increases the signal transmission rate, which is already high. A method that incorporates data scrambling is employed to address this issue at large data rates. In the section that follows, we look at two applications of this strategy.

Hence, multilevel binary schemes may effectively modify NRZ codes to solve their issues. There is a compromise, of course, as with any engineering design choice. The line signal may adopt one of three levels in multilevel binary coding, but each signal element, which might represent bits of information, carries only one bit of information. Hence, NRZ coding is more effective than multilevel binary.

Another way to put it is that, in contrast to the signaling formats previously mentioned, the receiver of multilevel binary signals must be able to discriminate between three levels. As a result, with the same likelihood of bit error, the multilevel binary signal needs around 3 dB more signal strength than a two-valued signal. In other words, the bit error rate for NRZ codes is much lower than that for multilevel binary for a given signal-to-noise ratio. The NRZ codes' drawbacks are overcame by a different set of coding methods referred to as biphase. Manchester and differential Manchester are two of these methods that are often used.

A low-to-high transition represents a 1, while a high-to-low transition represents a 0.4. The midbit transition functions as both a clocking mechanism and data. The midbit transition is only used in differential Manchester to provide clocking. The existence of a transition at the start of a bit period indicates the encoding of a 0 whereas the lack of a transition indicates the encoding of a 1. The use of differential encoding is a further benefit of differential Manchester. Each bit time in a biphase approach must have at least one transition and sometimes even two[12], [13]. As a result, the maximum modulation rate is twice as high as for NRZ, necessitating a higher bandwidth.

CONCLUSION

Signal encoding techniques are used to convert analog signals into digital signals that can be transmitted, stored, and processed more efficiently. There are various signal encoding techniques, including pulse code modulation (PCM), differential pulse code modulation (DPCM), delta modulation (DM), and adaptive delta modulation (ADM), each with its own advantages and disadvantages. Signal encoding techniques play a crucial role in modern communication systems, and the appropriate choice of encoding technique can have a significant impact on the overall performance of the system. Understanding the characteristics of different encoding techniques and their trade-offs is essential for designing efficient and effective communication systems.

REFERENCES

[1] K. B. Kim, H. T. Leem, Y. H. Chung, and H. B. Shin, “Feasibility study of multiplexing method using digital signal encoding technique,” *Nucl. Eng. Technol.*, 2020, doi: 10.1016/j.net.2020.03.027.

[2] T. Hur, J. Bang, T. Huynh-The, J. Lee, J. I. Kim, and S. Lee, "Iss2Image: A novel signal-encoding technique for CNN-based human activity recognition," *Sensors (Switzerland)*, 2018, doi: 10.3390/s18113910.

[3] D. Auge, J. Hille, E. Mueller, and A. Knoll, "A Survey of Encoding Techniques for Signal Processing in Spiking Neural Networks," *Neural Processing Letters*. 2021. doi: 10.1007/s11063-021-10562-2.

[4] M. I. O. Souza, A. F. Da Mota, V. M. Pepino, J. P. Carmo, and B. H. V. Borges, "Multi-Purpose Microwave Biosensor Based on Signal Encoding Technique and Microfluidics for Improved Sensitivity," *IEEE Sens. J.*, 2021, doi: 10.1109/JSEN.2020.3033970.

[5] R. Q. Hamza, K. S. Rijab, and M. A. R. Hussien, "Efficient electrocardiogram signal compression algorithm using dual encoding technique," *Indones. J. Electr. Eng. Comput. Sci.*, 2022, doi: 10.11591/ijeecs.v25.i3.pp1529-1538.

[6] "Wireless Communications and Networks," 2020. doi: 10.1109/sst49455.2020.9264269.

[7] M. Angeline and S. Suja Priyadharsini, "Hybrid compression of biomedical ECG and EEG signals based on differential clustering and encoding techniques," *Int. J. Imaging Syst. Technol.*, 2021, doi: 10.1002/ima.22489.

[8] X. Y. Peng, R. Jung, T. Toncian, O. Willi, and J. H. Teng, "Distortion of the intense terahertz signal measured by spectral-encoding technique," *Appl. Phys. Lett.*, 2009, doi: 10.1063/1.3148674.

[9] L. Amundsen, F. Andersson, D. J. van Manen, J. O. A. Robertsson, and K. Eggenberger, "Multisource encoding and decoding using the signal apparition technique," *Geophysics*, 2018, doi: 10.1190/GEO2017-0206.1.

[10] U. Katscher, J. Lisinski, and P. Börnert, "RF encoding using a multielement parallel transmit system," *Magn. Reson. Med.*, 2010, doi: 10.1002/mrm.22439.

[11] D. Seo and H. Nam, "Deep RP-CNN for Burst Signal Detection in Cognitive Radios," *IEEE Access*, 2020, doi: 10.1109/ACCESS.2020.3023262.

[12] X. Y. Peng, X. H. Zhang, J. H. Teng, H. C. Guo, and Y. L. Foo, "To realize the optimal probe pulse length for detection of pulsed terahertz signal with spectral-encoding technique," *Appl. Phys. Lett.*, 2011, doi: 10.1063/1.3598405.

[13] X. Y. Peng, J. H. Teng, X. H. Zhang, and Y. L. Foo, "Distortion analysis of pulsed terahertz signal measured with spectral-encoding technique," *J. Appl. Phys.*, 2010, doi: 10.1063/1.3499639.

CHAPTER 9

DIGITAL DATA COMMUNICATION TECHNIQUES: A COMPARATIVE ANALYSIS OF MODULATION, MULTIPLEXING, AND CODING TECHNIQUES FOR HIGH-SPEED AND RELIABLE COMMUNICATION

Dr. Arvind Kumar Pal, Assistant Professor,
Department of Computer Science, Sanskriti University, Mathura, Uttar Pradesh, India,
Email id- arvind@sanskriti.edu.in

ABSTRACT:

Digital data communication techniques refer to the methods used to transfer data between digital devices over a communication channel. With the rise of the digital age, the need for efficient and secure data communication has become increasingly important. Digital data communication techniques can be broadly classified into two categories - wired and wireless communication. Wired communication techniques include various types of cabling systems, such as twisted pair, coaxial, and fiber optic cables. These techniques are widely used for high-speed data transfer over short and long distances, and they offer high levels of reliability, security, and cost-effectiveness.

KEYWORDS:

Cabling System, Communication, Digital, Technique, Fiber Optics.

INTRODUCTION

Digital data communication techniques refer to the methods used to transmit digital data between two or more devices or networks. Digital data refers to information that has been converted into binary form, i.e., a sequence of 1s and 0s, which can be transmitted over communication channels. These techniques involve the use of various technologies and protocols to ensure that data is transmitted accurately, quickly, and securely [1]–[3]. Modulation is the process of converting digital data into analog signals for transmission over communication channels. Digital data is typically in the form of a series of binary bits, which can only represent two states: 0 and 1. However, analog signals can represent a range of values, allowing for the transmission of more complex signals.

The most common forms of modulation are amplitude modulation (AM), frequency modulation (FM), and phase modulation (PM). In AM, the amplitude of the carrier wave is varied to represent the binary bits, while in FM, the frequency of the carrier wave is varied. In PM, the phase of the carrier wave is varied. Multiplexing is the process of combining multiple signals into a single signal for transmission over a single communication channel. This technique is used to increase the capacity of communication channels and reduce the cost of transmission [4].

There are several types of multiplexing techniques, including time-division multiplexing (TDM), frequency-division multiplexing (FDM), and wavelength-division multiplexing (WDM). In TDM, multiple signals are transmitted in sequential time slots, while in FDM, multiple signals are transmitted on different frequency channels. In WDM, multiple signals are transmitted on different wavelengths of light. Error Detection and Correction Error detection and correction techniques are used to ensure that digital data is transmitted accurately and reliably. There are

several types of error detection and correction techniques, including parity checking, checksums, and cyclic redundancy checks (CRC). Parity checking involves adding an extra bit to each byte of data to indicate whether the number of 1s in the byte is even or odd. If an error occurs during transmission, the receiver can detect the error by checking the parity bit.

Checksums involve adding up all the bytes of data and storing the result as a checksum. The receiver can then perform the same calculation and compare the result with the checksum to detect any errors. CRC is a more sophisticated technique that involves dividing the data into blocks and performing a complex mathematical calculation to generate a checksum. The receiver can then perform the same calculation and compare the result with the checksum to detect any errors. Network Protocols Network protocols are sets of rules and procedures that govern the transmission of digital data over a network.

These protocols ensure that data is transmitted efficiently, securely, and reliably. The most common network protocols include the Transmission Control Protocol/Internet Protocol (TCP/IP), User Datagram Protocol (UDP), and Hypertext Transfer Protocol (HTTP). TCP/IP is the most widely used network protocol and is the basis of the internet. It is a set of protocols that govern the transmission of data over the internet, including the addressing of devices, the routing of data packets, and the establishment and termination of connections. UDP is a simpler network protocol that is used for low-latency, real-time applications, such as online gaming and video conferencing. Unlike TCP/IP, UDP does not guarantee the delivery of data packets and does not establish connections. HTTP is the protocol used for transmitting data over the World Wide Web. It is used to request and transmit data between web servers and clients, including web browsers [5].

Transmission media refer to the physical pathways used to transfer digital signals between devices. There are two types of transmission media: guided and unguided. Guided media include copper wires, coaxial cables, and fiber-optic cables. Unguided media include radio waves, microwaves, and infrared. Copper wires are the most common type of guided media used for local area networks (LANs) and wide area networks (WANs). Coaxial cables are used for cable TV and broadband internet connections. Fiber-optic cables are used for high-speed internet connections and long-distance communication. Fiber-optic cables use light to transfer data, making them faster and more secure than copper and coaxial cables.

Unguided media, such as radio waves, microwaves, and infrared, are used for wireless communication. Radio waves are used for broadcasting radio and TV signals, while microwaves are used for satellite communication and wireless networks. Infrared is used for short-range wireless communication, such as remote control devices. Modulation is the process of encoding digital data onto an analog signal for transmission over a communication channel. There are three types of modulation techniques: amplitude modulation (AM), frequency modulation (FM), and phase modulation (PM). AM is the process of varying the amplitude of a carrier signal to represent digital data. AM is used for radio broadcasting and is susceptible to interference and noise. FM is the process of varying the frequency of a carrier signal to represent digital data. FM is used for high-fidelity audio and is less susceptible to interference and noise than AM. PM is the process of varying the phase of a carrier signal to represent digital data. PM is used for digital communication and is less susceptible to interference and noise than AM and FM.

DISCUSSION

The three chapters before this one have mostly focused on the aspects of data transmission, including the properties of data signals and transmission medium, signal encoding, and transmission performance. The focus is shifted from data transmission to data communications in this chapter. It takes a lot of collaboration for two devices connected by a transmission media to share data. Normally, bits of data are sent through the channel one at a time. Both the transmitter and the receiver must use the same timing (rate, length, and spacing) for these bits. In Section 6.1, the asynchronous and synchronous methods of time control are examined. We next examine the issue of bit mistakes [6], [7]. As we have seen, data transmission involves some degree of inaccuracy, and it is necessary to account for these flaws. The chapter first briefly discusses the differences between single-bit mistakes and burst errors before moving on to two methods for handling errors: error detection and error repair.

Appendix G examines the physical interface between data sending devices and the transmission line as a complement to the information in this chapter. Digital data devices often don't directly connect to and signal over the channel. Instead, a standardized interface that offers significant control over the interaction between the sending and receiving devices and the transmission line mediates this process. As opposed to I/O devices and internal computer signal channels, which typically use a parallel set of lines for data transmission, the focus of this book is on serial data transmission, which transfers data over a single signal path. Signaling components are delivered down the line one at a time during serial transmission [8].

Unless otherwise mentioned, we assume one bit per signaling element in the discussion that follows for simplicity. This simplification has no significant impact on the topic. The binary value is determined by sampling the incoming signal once per bit time throughout the receipt of digital data. One of the challenges in such a procedure is that different transmission impairments would contaminate the signal, resulting in sporadic mistakes. This issue is made worse by a time issue: The arrival time and length of each bit that is received must be known by the receiver in order for it to sample the incoming bits correctly. Let's say the sender just sends a continuous stream of data bits. The sender's clock controls how quickly the bits are delivered. One bit will be delivered every millisecond, as determined by the sender's clock, if data transmission is set at, for instance, 1 Mbps. The receiver will often make an effort to sample the medium in the middle of each bit period. The receiver will space out its samples by one bit of time.

The sample would take place once every If the transmitter's and receiver's clocks are not properly synchronized, there will be an issue if the receiver timings its samples using its own clock. The initial sample will be 0.01 of a bit time away from the bit centre if there is a drift of 1% (the receiver's clock is 1% faster or slower than the transmitter's clock). The bit centre is the distance between the beginning and end of the bit. The receiver can be in error after 50 or more samples because it is sampling in the incorrect bit time. If the transmitter emits a sufficiently lengthy stream of bits and no action is taken to synchronise the transmitter and receiver, the mistake will ultimately cause the receiver to be out of step with the transmitter. For minor timing discrepancies, the error would happen later.

Two methods are often used to achieve the necessary synchronization. Oddly enough, the first is referred to as asynchronous transmission. With this technique, the time issue is avoided by avoiding transmitting lengthy, unbroken streams of bits. Timing or synchronization only has to be kept up inside each character; at the start of every new character, the receiver has the chance

to resynchronize. The line between the transmitter and receiver is in an idle state when no character is being broadcast. The signaling element for binary 1 is the same as the definition of idle. As a result, idle would be the existence of a negative voltage on the line for NRZ-L signaling, which is used for asynchronous transmission. A start bit with the value binary 0 marks the start of a character. The 5 to 8 bits that make up the character itself come next [9].

The character's bits are conveyed starting with the least important bit. For instance, the parity bit, which is at the most important bit position for IRA characters, is often placed after the data bits. Depending on the convention being used, the transmitter sets the parity bit such that the total number of ones in the character, including the parity bit, is either even (even parity) or odd (odd parity). The stop element, which is a binary 1, is the last component. There is a minimum length required for the stop element, which is typically 1, 1.5, or 2 times the length of an ordinary bit. There is no maximum value mentioned. The transmitter will keep sending the stop element until it is prepared to send the next character since the stop element and the idle condition are identical.

This plan has reasonable time requirements. As an example, IRA characters are often sent in 8-bit chunks that include the parity bit. The sample will change if the receiver is 5% faster or slower than the transmitter. Indeed, a mistake like the one I just mentioned leads to two mistakes. The last sampled bit is first received wrongly. Second, the bit count may not be aligned right now. Bit 8 could be misinterpreted for a start bit if bit 7 is a 1 and bit 8 is a 0. As the character, together with the start bit and end element, is frequently referred to as a frame, this circumstance is known as a framing mistake. A framing error may also happen if a noise situation makes a start bit appear in error when the system is idle.

Asynchronous transmission is easy and inexpensive, but it adds two to three overhead bits for each character. With an 8-bit character without a parity bit and a 1-bit-long stop element, for instance, two out of every 10 bits do not carry any information and are just there for synchronization; this results in a 20% cost. Of course, transmitting bigger blocks of bits between the start bit and stop element would lower the percentage overhead. The cumulative timing inaccuracy, however, increases with the size of the block of bits. Synchronous transmission is a distinct kind of synchronization that is utilized to gain higher efficiency.

A block of bits is broadcast in a continuous stream without start or stop codes while using synchronous transmission. The block may span many bits. It is necessary to synchronize the clocks of the transmitter and receiver in order to avoid time drift between them. One option is to provide the transmitter and receiver their own clock lines. One side either the broadcaster or the receiver periodically pulses the line with one brief pulse per bit time.

These consistent pulses serve as a clock for the other side. This method performs well over short distances, but timing problems may happen over longer distances because the clock pulses are subject to the same limitations as the data stream. The third option is to include the clocking data into the data stream. This may be done using Manchester or differential Manchester encoding for digital signals. Many methods may be used to analogue signals, such as synchronizing the receiver with the carrier frequency depending on the carrier phase.

Another degree of synchronization is needed with synchronous transmission so that the receiver can identify the start and stop of a block of data. Each block starts with a preamble bit pattern and often concludes with a post amble bit pattern to accomplish this. Additional bits are also

added to the block, which transmit control data utilized data connection control operations. A frame is made up of the data as well as the preamble, post amble, and control information. The data connection control mechanism being employed determines the actual frame format.

A generic representation of a typical frame format for synchronous transmission. The frame typically begins with an 8 bit long preamble called a flag. The post amble also uses the same flag. To indicate the beginning of a frame, the receiver watches for the flag pattern to appear. This is followed by a number of control fields that provide information on the data link control protocol, a data field that is variable in length for most protocols, further control fields, and finally a repetition of the flag.

Synchronous transmission is much more effective than asynchronous for large data blocks. Asynchronous transmission needs overhead of at least 20%. In synchronous transmission, the control data, preamble, and post amble are generally fewer than 100 bits. When a bit changes between transmission and receipt in digital transmission systems for example, when a binary 1 is broadcast but a binary 0 is received, or vice versa an error has occurred. Single-bit mistakes and burst errors are the two main categories of errors that might happen. An isolated error event known as a single-bit error modifies one bit but has no impact on the bits around it. A continuous sequence of B bits that contains a burst error of length B is one in which the initial and end bits as well as any number of the intermediate bits are received incorrectly.

An error burst is a collection of bits where two consecutive incorrect bits are never separated by more than x right bits. As a result, x right bits or more separate the final incorrect bit in one burst from the first incorrect bit in the burst that follows. As a result, there is a group of bits that experience a lot of mistakes during an error burst, however not necessarily every bit in the group experiences an error. When there is white noise present, a single-bit mistake may happen when the signal-to-noise ratio randomly deteriorates just enough to throw off the receiver's interpretation of a single bit. Burst mistakes are more frequent and more difficult to handle.

In today’s world, digital data communication techniques have become an essential part of our daily lives. Digital data communication refers to the transfer of digital information between two or more devices using a communication medium such as cables, optical fibers, wireless channels, or satellite links. These techniques have revolutionized the way we communicate and share information across the globe, enabling us to access vast amounts of information and connect with people and resources from anywhere in the world [10]. In this discussion, we will explore the various digital data communication techniques, their applications, advantages, and challenges.

Digital data communication techniques can be broadly categorized into two types: analog and digital communication. Analog communication refers to the transfer of signals that are continuous in nature, whereas digital communication involves the transfer of discrete signals[11]. In digital communication, data is encoded and transmitted as a series of 0s and 1s (bits). The following are some of the commonly used digital data communication techniques:

PCM is a technique used to digitally represent analog signals. It involves sampling the analog signal at regular intervals and quantizing each sample to a fixed number of bits. PCM is widely used in digital telephony systems, where it allows for high-quality voice transmission. TDM is a technique used to transmit multiple signals over a single communication channel. It works by dividing the channel into multiple time slots, each of which is allocated to a specific signal. TDM is commonly used in digital telephony and digital television systems.

FDM is a technique used to transmit multiple signals over a single communication channel by allocating each signal to a different frequency band. FDM is commonly used in radio and television broadcasting systems. Spread spectrum techniques are used to spread the transmission of a signal over a wider bandwidth than the signal would normally occupy. This makes the signal more resistant to interference and allows multiple signals to

CONCLUSION

Digital data communication techniques have revolutionized the way we transmit information across different devices and networks. There are several different techniques and technologies that enable digital data communication, including modulation schemes, error correction codes, multiplexing techniques, and routing protocols. The key advantages of digital data communication techniques is the ability to transmit large amounts of data quickly and reliably, even over long distances. This has made it possible to create a vast network of interconnected devices, from personal computers to smartphones to IoT devices.

REFERENCES

[1] J. M. Wier, “Digital Data Communication Techniques,” *Proceedings of the IRE*. 1961. doi: 10.1109/JRPROC.1961.287789.

[2] S. J. Kaur, L. Ali, M. K. Hassan, and M. Al-Emran, “Adoption of digital banking channels in an emerging economy: exploring the role of in-branch efforts,” *J. Financ. Serv. Mark.*, 2021, doi: 10.1057/s41264-020-00082-w.

[3] U. Jayasankar, V. Thirumal, and D. Ponnurangam, “A survey on data compression techniques: From the perspective of data quality, coding schemes, data type and applications,” *Journal of King Saud University - Computer and Information Sciences*. 2021. doi: 10.1016/j.jksuci.2018.05.006.

[4] A. Nasirahmadi and O. Hensel, “Toward the Next Generation of Digitalization in Agriculture Based on Digital Twin Paradigm,” *Sensors*. 2022. doi: 10.3390/s22020498.

[5] A. S. Krishen, Y. K. Dwivedi, N. Bindu, and K. S. Kumar, “A broad overview of interactive digital marketing: A bibliometric network analysis,” *Journal of Business Research*. 2021. doi: 10.1016/j.jbusres.2021.03.061.

[6] Y. Theocharis and A. Jungherr, “Computational Social Science and the Study of Political Communication,” *Polit. Commun.*, 2021, doi: 10.1080/10584609.2020.1833121.

[7] B. S. Pambudi and S. Suyono, “DIGITAL MARKETING AS AN INTEGRATED MARKETING COMMUNICATION STRATEGY IN BADAN USAHA MILIK DESA (BUMDesa) IN EAST JAVA,” *Competence J. Manag. Stud.*, 2020, doi: 10.21107/kompetensi.v13i2.6829.

[8] B. Carpentieri, “Efficient compression and encryption for digital data transmission,” *Secur. Commun. Networks*, 2018, doi: 10.1155/2018/9591768.

[9] S. Zeb, A. Mahmood, S. A. Hassan, M. J. Piran, M. Gidlund, and M. Guizani, “Industrial digital twins at the nexus of NextG wireless networks and computational intelligence: A survey,” *Journal of Network and Computer Applications*. 2022. doi: 10.1016/j.jnca.2021.103309.

[10] Z. Ashfaq *et al.*, "A review of enabling technologies for Internet of Medical Things (IoMT) Ecosystem," *Ain Shams Engineering Journal*. 2022. doi: 10.1016/ j.asej.2021.101660.

[11] G. Gushevinalti, P. Suminar, and H. Sunaryanto, "TRANSFORMASI KARAKTERISTIK KOMUNIKASI DI ERA KONVERGENSI MEDIA," *Bricol. J. Magister Ilmu Komun.*, 2020, doi: 10.30813/bricolage.v6i01.2069.

CHAPTER 10

ANALOG TRANSMISSION: CHALLENGES AND ADVANCEMENTS IN ANALOG COMMUNICATION SYSTEMS FOR ROBUST AND EFFICIENT COMMUNICATION

Dr. Deepanshu Singh, Assistant Professor,
Department of Computer Science, Sanskriti University, Mathura, Uttar Pradesh, India,
Email id- deepanshu@sanskriti.edu.in

ABSTRACT:

Analog transmission is a method of sending electrical signals that represent continuous data, such as voice or video, over a communication channel. It has been widely used in telecommunications for many years, although digital transmission has largely replaced it in recent times. In analog transmission, the amplitude and frequency of the signal are continuously varied in proportion to the information being transmitted. This modulation process is used to impose the information onto a carrier wave that can be transmitted over a medium such as a wire, radio waves, or optical fibers. The main advantage of analog transmission is its ability to transmit high-quality audio and video signals with low latency, which is important in real-time applications such as broadcasting and telephone communication.

KEYWORDS:

Analog Transmission, Bandwidth, Broadcasting, Digital, Electrical Signals.

INTRODUCTION

Analog transmission is a type of communication that involves sending data signals through a physical medium, such as a wire or radio frequency, using continuous analog signals. These signals vary in amplitude, frequency, or phase, and can represent sound, images, or other information. Analog transmission was the primary method of communication for many years before digital transmission became popular [1]–[3]. In analog transmission, the message signal, which carries the information to be transmitted, is first transformed into an analog signal. This signal is then modulated onto a carrier signal, which is a high-frequency sine wave with a constant amplitude and frequency. The carrier signal serves as a medium for the message signal to travel through the transmission medium, such as a wire or air.

There are three main types of modulation used in analog transmission: amplitude modulation (AM), frequency modulation (FM), and phase modulation (PM). AM involves varying the amplitude of the carrier wave to represent the message signal. FM involves varying the frequency of the carrier wave to represent the message signal. PM involves varying the phase of the carrier wave to represent the message signal [4]. Amplitude modulation (AM) is the simplest form of modulation used in analog transmission. In this method, the amplitude of the carrier signal is varied in proportion to the amplitude of the message signal. The resulting signal is called an amplitude-modulated signal. This signal is then transmitted through the physical medium. The receiver then demodulates the signal to recover the original message signal.

Frequency modulation (FM) is another popular form of modulation used in analog transmission. In this method, the frequency of the carrier signal is varied in proportion to the amplitude of the message signal. The resulting signal is called a frequency-modulated signal. This signal is then transmitted through the physical medium. The receiver then demodulates the signal to recover the original message signal. Phase modulation (PM) is similar to frequency modulation in that it varies the carrier wave, but it does so by changing the phase of the wave instead of the frequency. The phase of the carrier wave is shifted by an amount that corresponds to the amplitude of the message signal. This results in a signal called a phase-modulated signal, which is then transmitted through the physical medium. The receiver then demodulates the signal to recover the original message signal.

Analog transmission has some advantages over digital transmission. One advantage is that analog signals can transmit an infinite range of values, making it ideal for transmitting continuous signals, such as sound or video. Another advantage is that analog transmission is less susceptible to interference from electromagnetic fields, which can cause errors in digital transmissions. Additionally, analog transmission is easier and less expensive to implement than digital transmission, making it an attractive option for some applications [5]. However, analog transmission also has several disadvantages. One disadvantage is that analog signals degrade over long distances, which can cause distortion and noise in the transmitted signal. Additionally, analog signals are susceptible to noise and interference from other signals and electromagnetic fields, which can cause errors in the transmitted signal. Finally, analog transmission is not as efficient as digital transmission, as it requires more bandwidth to transmit the same amount of information.

Analog transmission is a type of communication that involves sending data signals through a physical medium using continuous analog signals. It has advantages over digital transmission, such as the ability to transmit an infinite range of values and resistance to interference, but it also has disadvantages, such as signal degradation over long distances and susceptibility to noise and interference. Analog transmission is still used in some applications, such as radio broadcasting and telephone communication, but digital transmission has largely replaced it in many other areas.

- **Applications of Analog Transmission:** Analog transmission has been used in many applications over the years, including radio and television broadcasting, telephone communication, and early computer networking. It is still used in some applications today, such as in certain types of industrial control systems, and in some areas of the world where digital infrastructure is not yet widely available.
- **Transmission Mediums:** Analog signals can be transmitted through various types of physical media, such as copper wire, fiber optic cables, and radio waves. Each medium has its own advantages and disadvantages, such as speed, range, and susceptibility to interference.
- **Crosstalk and Interference:** Analog transmission is susceptible to crosstalk, which occurs when signals from one transmission line are picked up by another nearby line. This can cause interference and distortion in the transmitted signal. Other types of interference, such as noise and electromagnetic interference, can also affect analog signals.

- **Bandwidth:** Analog transmission requires more bandwidth than digital transmission to transmit the same amount of information. This is because analog signals are continuous and can take on an infinite number of values, whereas digital signals are discrete and can only take on a finite number of values.
- **Modulation Techniques:** Modulation techniques can vary depending on the type of analog transmission being used. For example, amplitude modulation (AM) can be used for voice transmissions, while frequency modulation (FM) is often used for music and other high-fidelity audio transmissions. Phase modulation (PM) is commonly used in digital communication systems, such as satellite communication and wireless networks.
- **Signal Degradation:** Analog signals degrade over long distances, which can cause distortion and noise in the transmitted signal. This is because the signal loses power as it travels, which can result in a weaker signal at the receiver. Signal amplifiers can be used to boost the signal strength, but this can also introduce additional noise and distortion.

DISCUSSION

Analog transmission refers to the transfer of analog signals, which are continuous and infinitely variable, over a communication medium such as a wire or radio frequency. These signals can carry voice, music, video, and other types of data. Analog transmission is widely used in communication systems such as radio and television broadcasting, telephony, and cable television. In this article, we will explore the principles of analog transmission and the techniques used for signal modulation, transmission, and reception.

In analog transmission, the information signal is modulated onto a carrier wave, which is a high-frequency signal that can travel over a communication medium. Modulation is the process of varying the amplitude, frequency, or phase of the carrier wave in proportion to the information signal.

There are three main types of modulation techniques used in analog transmission: amplitude modulation (AM), frequency modulation (FM), and phase modulation (PM). In amplitude modulation, the amplitude of the carrier wave is varied in proportion to the amplitude of the information signal. The resulting modulated signal has a frequency equal to the frequency of the carrier wave, and the amplitude of the modulated signal varies over time. The basic formula for AM is:

$$S(t) = [1 + m(t)] \cos(2\pi fact)$$

Where s (t) is the modulated signal, m (t) is the information signal, fact is the carrier frequency, and cos (2πfact) is the carrier wave. The blue wave represents the information signal, and the red wave represents the modulated signal. In frequency modulation, the frequency of the carrier wave is varied in proportion to the amplitude of the information signal. The resulting modulated signal has a constant amplitude and a frequency that varies over time. The basic formula for FM is:

$$S(t) = \cos[2\pi f\_ct + k\_f \int m(\tau)\, d\tau]$$

Where s(t) is the modulated signal, m(t) is the information signal, fact is the carrier frequency, kef is the frequency sensitivity constant, and $\int m(\tau)\, d\tau$ is the integral of the information signal. The blue Internet Control Message Protocol wave represents the information signal, and the red wave represents the modulated signal.

Phase Modulation (PM)

In phase modulation, the phase of the carrier wave is varied in proportion to the amplitude of the information signal. The resulting modulated signal has a constant amplitude and a phase that varies over time. The basic formula for PM is:

$$s(t) = \cos[2\pi f\_ct + k\_p\, m(t)]$$

Where s(t) is the modulated signal, m(t) is the information signal, f_c is the carrier frequency, k_p is the phase sensitivity constant, and m(t) is the information signal.

Once the signal has been modulated, it needs to be transmitted over a communication medium. The choice of communication medium depends on the application and the distance over which the signal needs to be transmitted. A wire can be used to transmit signals over short distances, such as within a building or Analog and digital transmission are two different methods of transmitting data signals. Analog transmission uses continuous signals that vary in amplitude, frequency, or phase, while digital transmission uses discrete signals that represent binary data. Digital transmission offers several advantages over analog transmission, such as increased reliability and efficiency, but it is also more complex and expensive.

1. Analog-to-digital conversion (ADC) is the process of converting analog signals to digital signals. This is necessary when using digital equipment to process analog signals, such as in digital audio or video recording. ADCs work by sampling the analog signal at regular intervals and converting each sample to a digital value. The number of samples per second, or sample rate, determines the resolution and quality of the digital signal.
2. Digital-to-analog conversion (DAC) is the process of converting digital signals to analog signals. This is necessary when using digital equipment to play back analog signals, such as in digital audio or video playback. DACs work by converting each digital value to a corresponding analog voltage or current. The quality of the analog signal depends on the resolution and accuracy of the DAC.

Analog signal processing is the manipulation of analog signals using various techniques, such as filtering, amplification, and modulation. This can be used to improve the quality of analog signals or to extract specific information from the signal. Analog signal processing is used in many applications, such as audio and video processing, and can be implemented using analog circuits or digital signal processing techniques.Multiplexing is the process of combining multiple signals onto a single transmission line. This can be done using various techniques, such as frequency-division multiplexing (FDM), time-division multiplexing (TDM), or code-division multiplexing (CDM). Multiplexing is used in many applications to increase the efficiency of transmission lines and can be used with both analog and digital signals.

Digital-to-analog conversion, as the name suggests, is the process of converting digital data to a band pass analogue signal. Analog-to-analog conversion is the term used to describe the transformation of a low-pass analogue signal into a band pass analogue signal. We talk about these two different conversions in this chapter. The practice of altering an aspect of an analogue signal based on information in digital data is known as digital-to-analog conversion. The connection between the digital data, the digital-to-analog modulation process, and the resulting analogue signal. A sine wave is described by three properties: amplitude, frequency, and phase [6], [7].

Each of these features may be changed to produce a different wave. So, we may utilise a basic electric signal to represent digital data by altering one of its properties. We have at least three methods for converting digital data into an analogue signal: amplitude shift keying (ASK), frequency shift keying (FSK), and phase shift keying. Any of the three qualities may be changed in this manner (PSK). Moreover, there is a fourth (and superior) technique known as quadrature amplitude modulation that combines amplitude and phase changes (QAM). The most used technique nowadays is QAM, which is also the most effective of these alternatives. Prior to delving into particular digital-to-analog modulation techniques, it is important to understand two fundamental concepts: bit and baud rates, as well as the carrier signal.

The smallest unit of information that may be communicated, the bit, is what we used to describe a data element. The smallest constant unit of a signal is what we also defined as a signal element. Despite the fact that we continue to use the same terminology throughout this chapter, we will see that the nature of the signal element in analogue transmission is somewhat different. Like we did with digital transmission, we may determine the data rate (bit rate) and the signal rate (baud rate). They have a S=Nx connection with one another. Where r is the quantity of data items carried in a single signal element and N is the data rate (bps). In analogue transmission, the value of r is given by the formula r = log2 L, where L denotes the kind of signal element, not its level. To make the comparisons easier, the same terminology is used. ASK in binary (BASK)

ASK is often implemented using just two levels, despite the fact that we may have several levels (kinds) of signal components, each with a variable amplitude. On-off keying or binary amplitude shift keying are the terms used to describe this (OOK). One signal level's peak amplitude is zero, while the other is equal to the carrier frequency's peak amplitude[8].

Despite the fact that the carrier signal is only a single straightforward sine wave, modulation results in a composite no periodic signal. This signal contains a constant range of frequencies, as was mentioned. The bandwidth and signal rate are inversely related, as expected (baud rate). Nevertheless, another element termed d that relies on the modulation and filtering processes is often present. D's value ranges from 0 to 1. As a result, the bandwidth may be stated as in the, where 5 represents the signal rate and B the bandwidth.

$$B = (1 + d) \times S$$

According to the calculation, the necessary bandwidth ranges from 5 to a maximum of 25. The placement of the bandwidth is the most crucial factor in this situation the carrier frequency, is situated in the center of the bandwidth. This implies that we may pick our Ie such that the modulated signal fills a certain band pass channel if one is available. In actuality, this is the most significant benefit of digital-to-analog conversion. The resultant bandwidth may be adjusted to fit the available bandwidth.

Implementation the scope of this book does not allow for a thorough examination of ASK implementation. The straightforward principles that underlie the execution, however, could aid in our understanding of the notion itself. If the unipolar NRZ digital signal used to represent digital data has a high voltage of I V and a low voltage of 0 V, the implementation may be done by multiplying the NRZ digital signal by the carrier signal produced by an oscillator. When the NRZ signal's amplitude is 1, the carrier frequency's amplitude is in frequency shift keying, data is represented by changing the carrier signal's frequency. Over the period of one signal element, the modulated signal's frequency remains constant; however, if the data element changes, the

frequency changes for the subsequent signal element. For all signal components, the peak amplitude and phase stay constant[9].

Consideration of two carrier frequencies is one approach to conceptualizing binary FSK (or BFSK). We have chosen two carrier frequencies, f and 12. If the data element is 0, we utilise the first carrier; if it is 1, we use the second carrier. But, keep in mind that this is a fictitious scenario that is simply being used to illustrate the point. The difference between the carrier frequencies is often quite tiny and the carrier frequencies are relatively high. Broadband for BFSK is the FSK bandwidth. Once again, the carrier signals are just straightforward sine waves, but modulation results in the creation of a nonperiodic composite signal with continuous frequencies. The two ASK signals that make up FSK each have their own carrier frequency (Cil orh). If there is a 211j Hz difference between the two frequencies, then B=(l+d)xS+2iij Hz is the necessary bandwidth.

What ought to be 211/'s minimum value? We selected a number larger than (l + d)S. It can be shown that for modulation and demodulation to function correctly, the minimum value must be at least S. Implementation BFSK has both coherent and no coherent implementations. As one signal element finishes and the next starts, there could be a phase discontinuity in no coherent BFSK. Coherent BFSK maintains phase during the intersection of two signal components. By considering BFSK as two ASK modulations and using two carrier frequencies, no coherent BFSK may be constructed.

One voltage-controlled oscillator (VeO), which changes its frequency in response to the input voltage, may be used to achieve coherent BFSK. The principle underlying the second approach. The unipolar NRZ signal serves as the oscillator's input. The oscillator maintains its normal frequency while the NRZ amplitude is negative; when it is positive, the frequency is raised. The two signal components in binary PSK, one with a phase of 0° and the other with a phase of 180°, are the only ones present. Binary PSK is as straightforward as binary ASK, but it has one major benefit over ASK: it is less nal; in PSK, it is the phase. Noise is more likely to modify the amplitude than the phase. In other words, compared to ASK, PSK is less sensitive to noise. Since we do not require two carrier signals, PSK is better than FSK. The BPSK bandwidth. While it is smaller than for BFSK, the bandwidth is the same as for binary ASK. For the purpose of splitting two carrier signals, no bandwidth is lost. Implementation Similar to how ASK is implemented, BPSK is also straightforward. Since the signal element with phase 180° may be seen as the complement of the signal element with phase 0°, this is the explanation. This provides us with information on how to apply BPSK.

The same strategy we did for ASK but with a polar NRZ signal rather than a unipolar NRZ signal. The 1 bit (positive voltage) is represented by a phase beginning at 0°, and the abit (negative voltage) is represented by a phase starting at 180°. The polar NRZ signal is multiplied by the carrier frequency. Since BPSK is so straightforward, designers were drawn to employ 2 bits at a time in each signal element, which reduced the baud rate and ultimately the needed bandwidth. Since it employs two distinct BPSK modulations, one of which is in-phase and the other quadrature, the system is known as quadrature PSK or QPSK (out-of-phase). The incoming bits are first converted from serial to parallel, with the first bit going to one modulator and the second bit going to the other. Each bit supplied to the matching BPSK signal has a duration of 2T if each bit in the incoming signal has a length of T. This indicates that each BPSK signal's bit has a frequency that is one-half that of the original signal.

Each multiplier produces two composite signals that are sine waves with the same frequency but different phases. Another sine wave with one of four phases 45°, -45°, 135°, or -135° is produced when they are combined. We may transmit two bits per signal element (r = 2) since the output signal has four different types of signal components (L = 4). When employing two carriers, a constellation diagram may be very helpful in defining the amplitude and phase of a signal element one in-phase and one quadrature, whether working with multilevel ASK, PSK, or QAM, the figure is helpful. A signal element type is depicted as a dot in a constellation diagram. It often has the bit or set of bits that it can transport printed next to it.

Two axes make up the diagram. The in-phase carrier is tied to the horizontal X axis, whereas the quadrature carrier is related to the vertical Y axis. Four bits of information may be inferred for each spot on the diagram. The peak amplitude of the in-phase component is defined by the projection of the point on the X axis, and the peak amplitude of the quadrature component is defined by the projection of the point on the Y axis. The peak amplitude of the signal element (the sum of the X and Y components) is represented by the length of the line (vector) connecting the point to the origin; the signal element's phase is represented by the angle the line makes with the X axis. A constellation diagram makes it simple to find all the information we want.

This constraint reduces the possible bit rate. So far, we have only changed one of the three sine wave properties at a time, but what if we change both? Why not blend PSK with ASK? The principle underlying quadrature amplitude modulation is the use of two carriers, one in phase and the other quadrature, with differing amplitude levels for each carrier (QAM). Many QAM iterations are feasible. Several of these systems. The simplest 4-QAM method (four distinct signal element types) employing a unipolar NRZ signal to modulate each carrier. The method utilised for ASK was the same (OOK). Another 4-QAM employing polar NRZ is shown in Part B, although this one is identical to QPSK. Another QAM-4 is shown in part c, where the two carriers were each modulated by a signal with two positive values.

Displays an eight-level (16-QAM) constellation of a signal, with four positive and four negative levels. The representation of analogue information by an analogue signal is known as analog-to-analog conversion, also known as analogue modulation. Why modulate an analogue signal when it is already analogue, one could wonder. If the medium is bandpass in nature or if we only have access to a bandpass channel, modulation is required. Radio is one instance. Each radio station is given a certain amount of bandwidth by the government. Every station generates a low-pass signal in the same frequency band. The low-pass signals must be adjusted, each to a different range, to enable listening to several stations.

Amplitude modulation (AM), frequency modulation (FM), and phase modulation are the three methods for converting from analogue to analogue (PM). Often, FM and PM are grouped together. In FM transmission, the frequency of the carrier signal is modulated to match the modulating signal's changing voltage level (amplitude). The peak amplitude and phase of the carrier signal are constant, but as the information signal's amplitude varies, so does the carrier's frequency. The relationships between the modulating signal, the carrier signal, and the resulting FM signal.

CONCLUSION

Analog transmission is a method of transmitting data signals that has been used for many years in a variety of applications, such as radio and television broadcasting, telephone communication,

and early computer networking. Analog transmission uses continuous signals that vary in amplitude, frequency, or phase, and can be transmitted through various types of physical media, such as copper wire, fiber optic cables, and radio waves[10], [11]. While analog transmission has been largely replaced by digital transmission in many areas due to its superior efficiency and reliability, it still has valuable applications in certain areas where digital infrastructure is not yet widely available. Analog transmission continues to be a valuable tool for transmitting information and will likely continue to be used in certain applications for years to come.

REFERENCES

[1] Y. Gui, H. Lu, X. Jiang, F. Wu, and C. W. Chen, "Compressed Pseudo-Analog Transmission System for Remote Sensing Images over Bandwidth-Constrained Wireless Channels," *IEEE Trans. Circuits Syst. Video Technol.*, 2020, doi: 10.1109/TCSVT.2019.2935127.

[2] M. M. Amiri, D. Gunduz, S. R. Kulkarni, and H. V. Poor, "Convergence of Federated Learning over a Noisy Downlink," *IEEE Trans. Wirel. Commun.*, 2022, doi: 10.1109/TWC.2021.3103874.

[3] Y. Du and K. Huang, "Fast Analog Transmission for High-Mobility Wireless Data Acquisition in Edge Learning," *IEEE Wirel. Commun. Lett.*, 2019, doi: 10.1109/LWC.2018.2876344.

[4] J. Zhao, R. Xiong, and J. Xu, "OmniCast: Wireless Pseudo-Analog Transmission for Omnidirectional Video," *IEEE J. Emerg. Sel. Top. Circuits Syst.*, 2019, doi: 10.1109/JETCAS.2019.2898750.

[5] X. W. Tang, X. L. Huang, F. Hu, and Q. Shi, "Human-Perception-Oriented Pseudo Analog Video Transmissions with Deep Learning," *IEEE Trans. Veh. Technol.*, 2020, doi: 10.1109/TVT.2020.3003478.

[6] P. Li, F. Yang, J. Zhang, Y. Guan, A. Wang, and J. Liang, "Synthesis-Distortion-Aware Hybrid Digital Analog Transmission for 3D Videos," *IEEE Access*, 2020, doi: 10.1109/ACCESS.2020.2990198.

[7] M. Zbili and D. Debanne, "Past and future of analog-digital modulation of synaptic transmission," *Frontiers in Cellular Neuroscience*. 2019. doi: 10.3389/fncel.2019.00160.

[8] X. Jiang and H. Lu, "Joint rate and resource allocation in hybrid digital-analog transmission over fading channels," *IEEE Trans. Veh. Technol.*, 2018, doi: 10.1109/TVT.2018.2857515.

[9] W. Liu, Q. Liu, R. A. Crozier, and R. L. Davis, "Analog transmission of action potential fine structure in spiral ganglion axons," *J. Neurophysiol.*, 2021, doi: 10.1152/jn.00237.2021.

[10] X. W. Tang and X. L. Huang, "A Design of SDR-Based Pseudo-analog Wireless Video Transmission System," *Mob. Networks Appl.*, 2020, doi: 10.1007/s11036-020-01592-6.

[11] C. Lan, C. Luo, W. Zeng, and F. Wu, "A Practical Hybrid Digital-Analog Scheme for Wireless Video Transmission," *IEEE Trans. Circuits Syst. Video Technol.*, 2018, doi: 10.1109/TCSVT.2017.2671417.

CHAPTER 11

BANDWIDTH UTILIZATION: A COMPARATIVE STUDY OF MULTIPLEXING AND SPREADING TECHNIQUES FOR EFFICIENT AND SECURE DATA TRANSMISSION

Neeraj Kaushik, Assistant Professor
Department of Electronics and Communication Engineering, Teerthanker Mahaveer University, Moradabad, Uttar Pradesh, India
Email Id- neeraj1604@gmail.com

ABSTRACT:

Bandwidth utilization is the process of optimizing the use of available network bandwidth to transmit data efficiently and effectively. In computer networking, bandwidth is a limited resource that must be shared among multiple users and applications. To make the most efficient use of available bandwidth, various techniques can be used, such as compression, caching, traffic shaping, and Quality of Service (QoS) controls. Compression techniques reduce the size of data packets by removing redundant information, allowing more data to be transmitted in a given amount of time. Caching involves storing frequently accessed data locally, reducing the need for data to be transmitted over the network. Traffic shaping and QoS controls prioritize certain types of traffic, ensuring that important data is given higher priority and minimizing the impact of lower-priority traffic on the network.

KEYWORDS:

Bandwidth, Caching, Data Packets, Network, Traffic Shaping.

INTRODUCTION

Bandwidth utilization refers to the efficient use of available network bandwidth to transmit data. To maximize the use of bandwidth, various techniques are used, such as compression, caching, traffic shaping, and Quality of Service (QoS) controls. Two other important techniques for bandwidth utilization are multiplexing and spreading, which are used to increase the amount of data that can be transmitted over a given amount of bandwidth [1], [2]. Multiplexing is the process of combining multiple signals into a single signal for transmission over a shared medium. Multiplexing allows multiple users or applications to share the same bandwidth, reducing the need for additional bandwidth and improving network efficiency. There are several types of multiplexing techniques, including time-division multiplexing (TDM), frequency-division multiplexing (FDM), and wavelength-division multiplexing (WDM) [3].

Time-division multiplexing (TDM) is a technique in which multiple signals are transmitted sequentially over the same medium. In TDM, each signal is given a specific time slot during which it is transmitted. The time slots are allocated in a round-robin fashion, with each signal given an equal amount of time. TDM is used in many applications, including digital telephony, where multiple voice channels are combined into a single digital stream for transmission over a shared network. TDM is also used in digital video and audio applications, where multiple video or audio signals are combined into a single stream for transmission.

Frequency-division multiplexing (FDM) is a technique in which multiple signals are transmitted simultaneously over the same medium by allocating each signal a specific frequency band. In FDM, the signals are modulated onto different carrier frequencies and then combined for transmission over the same medium [4], [5]. FDM is used in many applications, including radio and television broadcasting, where multiple channels are transmitted simultaneously over the same frequency band. FDM is also used in cable television, where multiple channels are combined into a single cable for transmission to subscribers.

Wavelength-division multiplexing (WDM) is a technique in which multiple signals are transmitted simultaneously over the same fiber optic cable by allocating each signal a specific wavelength. In WDM, the signals are modulated onto different wavelengths of light and then combined for transmission over the same fiber optic cable [6]. WDM is used in many applications, including long-haul fiber optic transmission, where multiple channels are transmitted over the same fiber optic cable. WDM is also used in local area networks (LANs), where multiple signals are combined onto a single fiber optic cable for transmission between network devices.

Spread spectrum is a technique used to spread the bandwidth of a signal over a wider frequency range than the original signal. Spread spectrum is used to reduce interference and improve the reliability of wireless communication. There are two types of spread spectrum techniques: frequency-hopping spread spectrum (FHSS) and direct-sequence spread spectrum (DSSS). Frequency-hopping spread spectrum (FHSS) is a technique in which a signal is transmitted over multiple frequencies in a random sequence. In FHSS, the transmitter and receiver both follow the same frequency-hopping pattern, allowing them to synchronize their transmissions and receptions. FHSS is used in many wireless applications, including Bluetooth, wireless local area networks (WLANs), and military communication systems. FHSS provides improved resistance to interference and noise, as the signal is spread over multiple frequencies.

Bandwidth utilization refers to the effective use of available bandwidth in a communication system. With the increasing demand for high-speed data transmission and the limited bandwidth available, it is crucial to maximize bandwidth utilization. Multiplexing and spreading are two techniques used to increase bandwidth utilization in communication systems. Multiplexing is the process of transmitting multiple signals simultaneously over a single communication channel. There are several types of multiplexing techniques, including time-division multiplexing (TDM), frequency-division multiplexing (FDM), and wavelength-division multiplexing (WDM).

TDM is a technique that divides a communication channel into several time slots and allocates each slot to a different signal. In TDM, each signal is transmitted in a predetermined time slot, and the receiver reassembles the original signals from the received time slots. TDM is commonly used in telephone networks, where multiple voice signals are transmitted over a single communication line. FDM is a technique that divides a communication channel into several frequency bands and allocates each band to a different signal. In FDM, each signal is transmitted on a different frequency band, and the receiver separates the signals based on their frequency. FDM is commonly used in radio and television broadcasting, where multiple channels are transmitted simultaneously over the same communication medium.

WDM is a technique that divides a communication channel into several wavelengths and allocates each wavelength to a different signal. In WDM, each signal is transmitted on a different wavelength, and the receiver separates the signals based on their wavelength. WDM is

commonly used in fiber-optic networks, where multiple signals are transmitted over a single optical fiber. Multiplexing allows multiple signals to share a single communication channel, thereby increasing bandwidth utilization. However, it also introduces some challenges, such as signal interference and crosstalk, which can affect the quality of the transmitted signals [7], [8]. Spreading is another technique used to increase bandwidth utilization in communication systems. Spreading involves spreading a narrowband signal over a wideband communication channel. There are two types of spreading techniques: direct-sequence spreading and frequency-hopping spreading.

Direct-sequence spreading is a technique that spreads a narrowband signal over a wideband channel by multiplying it with a pseudorandom code. The pseudorandom code has a much higher data rate than the original signal, which spreads the signal over a wider frequency range. At the receiver, the pseudorandom code is multiplied with the received signal, which recovers the original signal. Direct-sequence spreading is commonly used in code-division multiple access (CDMA) systems, which allow multiple users to share the same frequency band.

Frequency-hopping spreading is a technique that spreads a narrowband signal over a wideband channel by hopping the carrier frequency of the signal over a predefined sequence of frequencies. The hopping sequence is determined by a pseudorandom code, which is synchronized between the transmitter and receiver. At the receiver, the signal is de-hopped by multiplying it with the same pseudorandom code used at the transmitter. Frequency-hopping spreading is commonly used in frequency-hopping spread-spectrum (FHSS) systems, which are used in military and satellite communications. Spreading allows multiple signals to share a wideband communication channel, thereby increasing bandwidth utilization. Spreading also provides some benefits, such as increased security and resistance to interference and jamming.

DISCUSSION

Bandwidth utilization through multiplexing and spreading, let's delve deeper into each technique and explore their advantages, challenges, and applications.

Multiplexing Techniques:

1. **Time-division multiplexing (TDM):**

TDM is a method of multiplexing where several signals share a single communication channel by dividing the channel into time slots. Each signal is allocated a predetermined time slot to transmit its data. At the receiver, the signals are reassembled by the demultiplexer. TDM is widely used in digital telephone networks, where multiple voice signals share a single communication line.

Advantages of TDM:

a) Efficient use of available bandwidth

b) No interference between signals

c) Low cost

Challenges of TDM:

a) Limited number of signals that can be transmitted

b) Clock synchronization issues between transmitter and receiver

2. Frequency-division multiplexing (FDM):

FDM is a method of multiplexing where several signals share a single communication channel by dividing the channel into different frequency bands. Each signal is allocated a different frequency band to transmit its data. At the receiver, the signals are separated by the de-multiplexer. FDM is commonly used in radio and television broadcasting.

Advantages of FDM:

a) Efficient use of available bandwidth

b) Allows different signals to be transmitted over the same communication channel

c) Simple implementation

Challenges of FDM:

a) Interference between signals

b) Limited bandwidth available for each signal

c) Requires precise tuning of frequency

3. Wavelength-division multiplexing (WDM):

WDM is a method of multiplexing where several signals share a single communication channel by dividing the channel into different wavelengths. Each signal is allocated a different wavelength to transmit its data. At the receiver, the signals are separated by the de-multiplexer. WDM is commonly used in fiber-optic networks, where multiple signals are transmitted over a single optical fiber.

Advantages of WDM:

a) Efficient use of available bandwidth

b) High data transmission rates

c) Allows different signals to be transmitted over the same communication channel

Challenges of WDM:

a) Expensive implementation

b) Requires precise wavelength control

c) Interference between signals

Spreading Techniques:

1. Direct-sequence spreading (DSS):

DSS is a method of spreading a narrowband signal over a wideband communication channel. The signal is multiplied by a pseudorandom code that has a much higher data rate than the original signal, which spreads the signal over a wider frequency range. At the receiver, the signal is despread by multiplying it with the same pseudorandom code used at the transmitter. DSS is commonly used in code-division multiple access (CDMA) systems.

Advantages of DSS:

a) Efficient use of available bandwidth

b) Provides high security

c) Resistant to interference and jamming

Challenges of DSS:

a) Requires precise synchronization of the pseudorandom code between transmitter and receiver

b) Susceptible to noise and multipath fading

2. Frequency-hopping spreading (FHS):

FHS is a method of spreading a narrowband signal over a wideband communication channel by hopping the carrier frequency of the signal over a predefined sequence of frequencies. The hopping sequence is determined by a pseudorandom code, which is synchronized between the transmitter and receiver. At the receiver, the signal is de-hopped by multiplying it with the same pseudorandom code used at the transmitter. FHS is commonly used in frequency-hopping spread-spectrum (FHSS) systems, which are used in military and satellite communications [9].

Advantages of FHS:

a) Efficient use of available bandwidth

b) Provides high security

c) Resistant to interference and jamming

Bandwidth monitoring is the process of measuring and analyzing the usage of network bandwidth. This is done to identify network performance issues, track the usage of network resources, and optimize network capacity. Bandwidth monitoring can be done using various tools, such as network traffic analyzers, packet sniffers, and bandwidth utilization software.

Bandwidth management is the process of allocating and prioritizing network bandwidth to different users and applications. This is done to ensure that critical traffic, such as voice and video, is given priority over less important traffic, such as email and web browsing. Bandwidth management can be done using various techniques, such as traffic shaping, Quality of Service (QoS) controls, and bandwidth throttling.

Bandwidth throttling is the intentional slowing down of network traffic to limit the amount of bandwidth used by certain applications or users. This is done to ensure that critical applications, such as voice and video, are not impacted by less important applications, such as file downloads and web browsing. Bandwidth throttling can be used to control network congestion and prevent network downtime.

Content Delivery Networks (CDNs) are networks of servers that are used to deliver web content to users. CDNs are designed to optimize the delivery of web content by caching and delivering content from servers that are geographically closer to the user. This can help to reduce latency and improve the performance of web applications. CDNs are used by many large organizations

to optimize the delivery of web content to users [10]. DSSS is used in many wireless applications, including wireless LANs and cellular phone networks. DSSS provides improved resistance to interference and noise, as the signal is spread over a wider bandwidth.

Code-division multiple access (CDMA) is a technique in which multiple users share the same frequency band by using different PN codes to spread their signals. In CDMA, each user is assigned a unique code that is used to spread their signal. The receiver can then despread the signal by using the same code. CDMA is used in many wireless applications, including cellular phone networks and satellite communication systems. CDMA provides improved resistance to interference and noise, as each user's signal is spread over the entire frequency band.

Orthogonal frequency-division multiplexing (OFDM) is a technique in which a signal is divided into multiple subcarriers, each with a different frequency and phase. In OFDM, the subcarriers are orthogonal to each other, meaning they are perfectly spaced apart and do not interfere with each other. OFDM is used in many applications, including digital television broadcasting, wireless LANs, and high-speed Internet access. OFDM provides improved resistance to interference and noise, as the subcarriers are orthogonal to each other and do not interfere with each other. Real-world connections have finite bandwidths. One of the biggest problems with electronic communications has been and will continue to be the appropriate utilization of these bandwidths. The application, however, may affect how wisdom is used. In order to utilize a channel with a bigger bandwidth, we may need to combine numerous low-bandwidth channels.

Sometimes increasing a channel's capacity is necessary to fulfil objectives like secrecy and ant jamming. These two major types of bandwidth utilization multiplexing and spreading are examined in this chapter. Our objective in multiplexing is efficiency; we merge numerous channels into one. We spread a channel's bandwidth to provide redundancy, which is required to meet our spreading objectives of secrecy and ant jamming. When a medium connecting two devices has more bandwidth than the devices themselves use, the connection might be shared. A single data connection may be used to simultaneously transmit numerous signals thanks to a group of methods called multiplexing [11].

The usage of data and communications also results in a rise in traffic. When a new channel is required, we may either build higher-bandwidth connections or utilize each to carry multiple signals, or we can continue to add individual links to account for the growth. Today's technology includes high-bandwidth media like optical fiber and microwaves from satellites and terrestrial sources. Each has a bandwidth that is much larger than what is required for the typical transmission signal. The bandwidth of a connection is wasted if it has more capacity than the linked devices really need. One of the most valuable resources we have in data transmission is bandwidth, thus an efficient system optimizes the use of all resources. N lines share a link's bandwidth in a multiplexed system. A multiplexed system's fundamental structure. A multiplexer (MUX) is where the lines on the left send their transmission streams so that it may combine them into one stream (many-tone). This stream is routed onto a DE multiplexer (DEMUX) at the receiving end, which divides it back into its individual transmissions (one-to-many) and routes them to the appropriate lines. The physical route is referred to as a link in the illustration. The section of a connection that transmits a transmission between a specific pair of lines is referred to as a channel.

There may be n channels on a single connection. When a link's (in hertz) bandwidth is larger than the sum of the bandwidths of the signals to be carried, frequency-division multiplexing

(FDM), an analogue method, may be used. Signals produced by each transmitting device modify a unique carrier frequency in FOM. A single composite signal that may be sent across the network is created by combining these modulated signals. There is enough bandwidth between the carrier frequencies to handle the modulated signal. The different signals' transmission channels fall within these bandwidth bands.

Channels may be divided using the multiplexing process is conceptually every source produces a signal with a corresponding frequency range. These comparable signals modify several carrier frequencies (/1,12, andh) within the multiplexer. After that, the resultant modulated signals are merged into a single composite signal and delivered across a media connection with sufficient bandwidth. The demultiplexer breaks down the multiplexed signal into its component signals using a series of filters. The demodulator then separates the constituent signals from their carriers and sends them to the output lines. In this analogue hierarchy, a group is created by multiplexing 12 voice channels onto a higher-bandwidth line. A group may handle 12 voice channels and 48 kHz of bandwidth.

At the next level, a supergroup a composite signal can be produced by multiplexing up to five groups. A supergroup may accommodate up to 60 voice channels and has a 240 kHz bandwidth. Supergroups may consist of 60 separate voice channels or five groups. Ten supergroups are multiplexed to form a master group at the next level. The minimum bandwidth required for a master group is 2.40 MHz, while the need for guard bands between supergroups raises the minimum bandwidth to 2.52 MHz. For master groups, 600 voice channels are supported. A jumbo group may be created by combining six master groups. In order to accommodate guard bands between the master groups, jumbo groups are supplemented to 16.984 MHz from their required 15.12 MHz (6 x 2.52 MHz). AM and FM radio transmission is a relatively popular FDM application. Air is the transmission medium for radio. AM radio has a dedicated band from 530 to 1700 kHz. This band must be shared by all radio stations.

Each AM station requires 10 kHz of bandwidth, as was covered. Each station shifts and multiplexes its broadcast since they each employ a different carrier frequency. The signal that is broadcast over the air is made up of many components. All of these signals are received by a receiver, but it only filters out the required signal through tuning. Just one AM station could transmit to the shared connection, the air, without multiplexing. We must understand that there is a physical multiplexer or demultiplexer present, however. FM broadcasting has a similar scenario. Since each station has a 200 kHz bandwidth, FM has a larger spectrum of 88 to 108 MHz. FDM is often used in television transmission. The bandwidth for each TV channel is 6 MHz. FDM is also used in the initial generation of cellular phones, which are still in use. Two 30-kHz channels are allotted to each user, one for speech transmission and the other for voice reception.

FM is used to modulate the speech signal, which has a 3 kHz bandwidth (from 300 to 3300 Hz). Note that the bandwidth of an FM signal is 10 times that of the modulating signal, therefore each channel has a bandwidth of 30 kHz (10 x 3). As a result, the base station provides each user with a 60-kHz bandwidth in the range that is accessible at the time of the call. WDM technology is quite sophisticated, yet the fundamental concept is fairly simple. At the multiplexer, we want to combine several light sources into a single light source, and at the demultiplexer, we want to do the opposite. A prism can readily manage the mixing and splitting of light sources. Remember from elementary physics that a prism bends a light beam dependent on the incidence angle and

frequency. This method allows a multiplexer to combine numerous input light beams, each with a small range of frequencies, into a single output beam with a larger spectrum of frequencies. The procedure may also be reversed using a demultiplexer. The SONET network, which multiplexes and demultiplexes multiple optical fibre lines, is one example of how WDM is used. By placing channels closely together, a new technique known as dense WDM (DWDM) may multiplex a very high number of channels. That succeeds even more effectively.

A digital technique called time-division multiplexing (TDM) enables numerous connections to share the high bandwidth of a line. Time is shared rather than a fraction of the bandwidth, as in FDM. Time in the link is spent on each connection. The identical connection that was utilised in FDM is employed here, but it is sectioned by time rather than by frequency. In the illustration, sections of signals 1, 2, 3, and 4 successively fill the connection. Notice that only multiplexing, not switching. This implies that each piece of information in a message from source 1 always travels to the same location, whether it is 1, 2, 3, or 4. Unlike switching, the delivery is constant and consistent.

One timeshared link contains digital material that has been integrated from many sources. The sources can still generate analogue data since it can be sampled, converted to digital data, and then multiplexed using TDM, therefore this is not to say that they cannot. TDM may be divided into synchronous and statistical systems. We first go over synchronous TDM before demonstrating how statistical TDM is different. Each input connection in synchronous TDM has an allocation in the output even if it is not providing data.

Each input connection's data flow in synchronous TDM is split into units, with each input taking up one input time slot. One bit, one character, or one data block may all be considered units. Every input unit transforms into an output unit and takes up a single output time slot. Yet, an output time slot's duration is n times shorter than an input time slots. When there are n connections and an input time slot is T s, the output time slot is Tin s. In other words, a unit in the output link moves more quickly and has a shorter duration.

A synchronous TDM example with n equal to 3 frame in synchronous TDM is made up of a round of data units from each input link will see the reason for this shortly. A frame is split into n time slots if there are n connections, and one slot is allotted for each unit and each input line. If the input unit lasts for time T, then each slot lasts for time Tin, and each frame lasts for time T unless a frame contains more information, as we will see in a moment.

To ensure the flow of data, the output link's data rate must be n times higher than the connection's data rate the link's data rate is three times that of a connection, and a unit's duration on a connection is three times that of a time slot duration of a unit on the link. The size of the data before multiplexing is shown in the graphic as being three times that of the data after multiplexing. Only to illustrate that each unit is three times greater in length before multiplexing than it is after. TDM implementation is more complex than FDM implementation. The multiplexer and DE multiplexer'ssynchronization is a significant problem.

A bit from one channel may be received by the incorrect channel if the multiplexer and the DE multiplexer are not synced. One or more synchronization bits are often inserted at the start of each frame as a result. Framing bits follow a pattern from frame to frame that synchronizes the DE multiplexer with the incoming stream and enables precise time slot separation this synchronization information typically consists of 1 bit every frame that alternates between 0 and

I. Each input in synchronous TDM has a reserved space in the output frame, as we saw in the previous section. If some input lines have no data to relay, this may not be efficient. Slots are dynamically assigned in statistical time-division multiplexing to increase bandwidth efficiency.

A slot in the output frame is only assigned to an input line when it contains data to deliver that would fill that slot. The number of slots in each frame in statistical multiplexing is smaller than the number of input lines. Each input line is checked by the multiplexer in a round-robin method; if a line contains data to deliver, it is given a slot; if not, it is skipped and the next line is checked. Since the relevant line does not have any data to convey, certain slots in the former are vacant. But, with the latter, no slot is left vacant as long as any input line has data that has to be delivered.

Another significant distinction between slots in synchronous TDM and statistical TDM. In synchronous TDM, data completely fills an output slot; in statistical TDM, a slot must hold both data and the destination's address. With synchronous TDM, synchronization and the previously established connections between the inputs and outputs act as addresses, therefore addressing is not necessary. For instance, we are aware that input 1 always connects to input 2. This is assured if the multiplexer and the DE multiplexer are synced. Since there are no reassigned or allocated slots in statistical multiplexing, there is no set link between the inputs and outputs. To indicate where it is to be sent, we must put the address of the recipient within each space. In its most basic form, addressing may be defined as N distinct output lines defined by n bits with n = 10g2 N. For instance, a 3-bit address is required for eight separate output lines.

In statistical TDM, a slot contains both data and an address, hence an acceptable data-to-address size ratio is necessary for effective transmission. For instance, sending 1 bit per slot as data when the address is 3 bits would be wasteful. A 300 percent overhead would result from this. A block of data in statistical TDM often has several bytes, while the address only has a few bytes. Another distinction between synchronous and statistical TDM exists, however this time it relates to the frames[12]. We do not require synchronization bits since the frames in statistical TDM do not need to be synced. In statistical TDM, the link's capacity is often smaller than the total of its channel capacities. Based on the statistics of the load for each channel, statistical TDM designers determine the link's capacity. The link's capacity represents the average input slot fill rate, which is x percent. Of course, some spaces must wait during busy periods.

CONCLUSION

Bandwidth utilization is a crucial aspect of modern communication systems. The efficient use of available bandwidth can have a significant impact on the overall performance, reliability, and cost-effectiveness of communication networks. Multiplexing and spreading are two important techniques used to maximize the use of available bandwidth. Multiplexing techniques allow multiple signals to be transmitted over the same medium, which reduces the need for additional bandwidth and improves network efficiency. On the other hand, spreading techniques such as FHSS, DSSS, CDMA, and OFDM, are used to spread the bandwidth of a signal over a wider frequency range, reducing interference and improving the reliability of wireless communication.

REFERENCES

[1] A. L. F. De Almeida and G. Favier, “Unified tensor model for space-frequency spreading-multiplexing (SFSM) MIMO communication systems,” *EURASIP J. Adv. Signal Process.*, 2013, doi: 10.1186/1687-6180-2013-48.

[2] W. Bai *et al.*, "Photonic Millimeter-Wave Joint Radar Communication System Using Spectrum-Spreading Phase-Coding," *IEEE Trans. Microw. Theory Tech.*, 2022, doi: 10.1109/TMTT.2021.3138069.

[3] K. Nagatomi, H. Kawai, and K. Higuchi, "Complexity-reduced MLD based on QR decomposition in OFDM MIMO multiplexing with frequency domain spreading and code multiplexing," *EURASIP J. Adv. Signal Process.*, 2011, doi: 10.1155/2011/525829.

[4] A. L. F. de Almeida, G. Favier, and J. C. M. Mota, "Space-time spreading-multiplexing for MIMO wireless communication systems using the PARATUCK-2 tensor model," *Signal Processing*, 2009, doi: 10.1016/j.sigpro.2009.04.028.

[5] A. R. Khan and S. M. Gulhane, "A highly sustainable multi-band orthogonal wavelet code division multiplexing UWB communication system for underground mine channel," *Digit. Commun. Networks*, 2018, doi: 10.1016/j.dcan.2017.09.007.

[6] S. S. Das and S. Tiwari, "Discrete Fourier transform spreading-based generalised frequency division multiplexing," *Electron. Lett.*, 2015, doi: 10.1049/el.2014.3833.

[7] X. Yu, B. Tong, B. Luanjian, Y. Guanghui, and H. Liujun, "A Novel Modulation and Multiplexing Technology for Reducing Out-of-Band Leakage Based on Multicarrier Schemes," *IEEE Access*, 2020, doi: 10.1109/ACCESS.2020.2985988.

[8] B. Ma, B. Li, X. Y. Wang, C. P. Wang, J. Li, and Y. Q. Shi, "Code division multiplexing and machine learning based reversible data hiding scheme for medical image," *Secur. Commun. Networks*, 2019, doi: 10.1155/2019/4732632.

[9] B. Ma, J. C. Hou, C. P. Wang, X. M. Wu, and Y. Q. Shi, "A reversible data hiding algorithm for audio files based on code division multiplexing," *Multimed. Tools Appl.*, 2021, doi: 10.1007/s11042-021-10532-9.

[10] Y. Ida, T. Matsumoto, and S. Matsufuji, "Different antenna interleaved allocation with full and divided WHT/DFT spreading for HTRCI-MIMO/OFDM," *IEICE Trans. Commun.*, 2020, doi: 10.1587/transcom.2019EBP3216.

[11] E. H. Kim, H. S. Kim, and K. W. Lee, "Range dividing MIMO waveform for improving tracking performance," *Sensors*, 2021, doi: 10.3390/s21217290.

[12] L. Dai, B. Wang, Y. Yuan, S. Han, C. L. I, and Z. Wang, "Non-orthogonal multiple access for 5G: Solutions, challenges, opportunities, and future research trends," *IEEE Commun. Mag.*, 2015, doi: 10.1109/MCOM.2015.7263349.

CHAPTER 12

TRANSMISSION MEDIA: A COMPREHENSIVE ANALYSIS OF WIRED AND WIRELESS COMMUNICATION CHANNELS FOR MODERN DATA COMMUNICATION SYSTEMS

Prashant Kumar, Assistant Professor
Department of Electronics and Communication Engineering, Teerthanker Mahaveer University, Moradabad, Uttar Pradesh, India
Email Id- tmu.iqac@gmail.com

ABSTRACT:

Transmission media refers to the physical pathways that carry signals from one device to another in a communication network. Guided transmission media include wired pathways such as twisted-pair copper wire, coaxial cable, and optical fiber. Twisted-pair copper wire is commonly used in local area networks (LANs) and telephone systems, while coaxial cable is often used in cable television and high-speed internet connections. Optical fiber, which uses light to transmit signals, is becoming increasingly popular due to its high bandwidth and resistance to interference. Unguided transmission media, also known as wireless transmission media, include air and space. This type of media includes radio waves, microwaves, and satellite communications. Wireless transmission media are often used in mobile devices, remote sensing systems, and wireless local area networks (WLANs).

KEYWORDS:

Communication Network, Optic Fiber, Internet Connection, Microwave, Wireless Area Network.

INTRODUCTION

Transmission media, also known as communication channels, refer to the physical pathways that carry communication signals between devices. Transmission media can be broadly classified into two categories: guided media and unguided media. Guided media are those that require a physical conduit to carry signals from one point to another. Examples of guided media include twisted pair cable, coaxial cable, and fiber optic cable. Unguided media, on the other hand, do not require a physical conduit and rely on air or vacuum to propagate signals. Examples of unguided media include radio waves, microwaves, and infrared waves [1], [2] .

Twisted pair cable is a type of cable that consists of two insulated copper wires twisted together to reduce electromagnetic interference (EMI) from external sources. Twisted pair cable is the most common type of cable used for communication in local area networks (LANs) and wide area networks (WANs). Twisted pair cable can be further divided into two types: shielded twisted pair (STP) and unshielded twisted pair (UTP). Coaxial cable is a type of cable that consists of a central conductor, an insulating layer, a conductive shield, and an outer jacket. The central conductor is typically made of copper and carries the signal, while the conductive shield reduces EMI from external sources. Coaxial cable is commonly used to transmit signals in cable television, broadband internet, and other high-speed data networks.

Fiber optic cable is a type of cable that consists of thin strands of glass or plastic fibers that transmit signals using light. Fiber optic cable is commonly used for long-distance communication and offers several advantages over other types of cables, including high bandwidth, low attenuation, and immunity to EMI. Radio waves are a type of electromagnetic radiation that are used for communication in radio and television broadcasting, wireless networks, and satellite communication. Radio waves have a relatively low frequency and long wavelength, which enables them to travel long distances without being significantly attenuated.

Microwaves are a type of electromagnetic radiation that have a higher frequency and shorter wavelength than radio waves. Microwaves are commonly used for communication in microwave ovens, mobile phone networks, and satellite communication. Infrared waves are a type of electromagnetic radiation that have a higher frequency and shorter wavelength than microwaves. Infrared waves are commonly used for communication in remote controls, optical fiber communication, and security systems.

Advantages and Disadvantages of Transmission Media:

Each type of transmission media has its own advantages and disadvantages. Here are some of the key advantages and disadvantages of each type of transmission media:

Guided Media:Advantages

a) Twisted Pair Cable:
b) Easy to install and terminate
c) Inexpensive
d) Good for short distances

Disadvantages:

a) Susceptible to EMI from external sources
b) Limited bandwidth

Coaxial Cable: Advantages:

a) High bandwidth
b) Good for long distances
c) Reduced susceptibility to EMI

Disadvantages:

a) Expensive
b) Difficult to install and terminate

Fiber Optic Cable: Advantages:

a) High bandwidth
b) Immune to EMI
c) Good for long distances

Disadvantages:

a) Expensive

b) Difficult to install and terminate

c) Fragile

Unguided Media:

Radio Waves: Advantages:

a) Can travel long distances without significant attenuation

b) Can penetrate through walls and other obstacles

c) Inexpensive

Disadvantages:

a) Limited bandwidth

b) Susceptible to interference from other sources

Microwaves

Advantages and Disadvantages of Transmission Media (continued):

Unguided Media (continued):

Microwaves: Advantages:

a) High bandwidth

b) Can travel long distances without significant attenuation

c) Can penetrate through walls and other obstacles

Disadvantages:

a) Expensive to install and maintain

b) Susceptible to interference from weather conditions, such as rain and snow

Infrared Waves: Advantages:

a) Inexpensive

b) Does not interfere with other signals

Disadvantages:

a) Limited range

b) Susceptible to interference from external sources, such as sunlight

The amount of data that can be transmitted over a given time period is determined by the bandwidth of the transmission medium. High-bandwidth media, such as fiber optic cable and

microwave, are required for transmitting large amounts of data quickly. The distance between the sender and receiver is a critical factor in determining the most appropriate transmission medium. Guided media, such as twisted pair and fiber optic cable, are suitable for long distances, while unguided media, such as radio waves and microwaves, are suitable for short distances.

The susceptibility of the transmission medium to external sources of interference, such as EMI and weather conditions, must be considered when selecting a medium. The cost of the transmission medium, including installation and maintenance costs, must be taken into account when making a selection. The reliability of the transmission medium is critical in determining the overall effectiveness of the communication system. Media with high reliability, such as fiber optic cable, are preferred over those with low reliability, such as radio waves.

DISCUSSION

Everything that can transmit information from a source to a destination falls within the general definition of a transmission medium. For instance, air serves as the communication channel for a dinner discussion between two individuals [3], [4]. With a smoke signal or semaphore, the message may also be sent via the air. The definition of the information and the transmission channel are more precise in data communications. Usually, open space, metallic cable, or fiber-optic cable serve as the transmission medium. Often, the information is a signal that results from converting data from another form.

When Morse created the telegraph in the 19th century, long-distance communication via electric impulses became a reality. Telegraph communication required a metallic medium and was sluggish. The invention of the telephone in 1869 made it feasible to increase the human voice's range. At the time, the electric signals produced by converting human speech into telephone signals required a metallic medium to transport them. Yet, the unstable communication was caused by the subpar wiring. The technology was basic, and the lines were often loud.

Hertz was able to transmit high frequency signals in 1895, which led to the beginning of wireless communication. Subsequently, Marconi developed a strategy for transmitting telegraph-like signals over the Atlantic. We have made great progress. There are now better metallic media available twistedpair and coaxial cables, for example. The data rate has dramatically risen because to the introduction of optical fibres. In part as a result of the technologies such as modulation and multiplexing outlined in the preceding chapters, free space (air, vacuum, and water) is utilised more effectively. Computers and other telecommunications equipment employ signals to represent data, signals are sent from one device to another via transmission medium in the form of electromagnetic radiation.

In addition to power, radio waves, infrared light, visible light, ultraviolet light, and X, gamma, and cosmic rays, electromagnetic energy also contains radio waves, visible light, and infrared light that vibrate in relation to one another. They all make up different parts of the electromagnetic spectrum. Nevertheless, not all of the spectrum's bands can now be used for communications. There are just a few different sorts of media that can be used to harness the useable ones [5].

Twisted-pair cable, coaxial cable, and fiber-optic cable are examples of guided media, which act as a conduit from one device to another. The physical boundaries of each of these mediums guide and confine a signal as it travels along them. Metallic (copper) conductors are used in

coaxial and twisted-pair cable to receive and convey signals in the form of electric current. A cable that absorbs and transmits messages in the form of light is called an optical fiber. The receiver receives signals on one of the lines, while the other wire serves merely as a ground reference. The receiver makes advantage of these differences. Crosstalk and interference (noise) may influence both lines in addition to the signal delivered on one of the wires by the sender and result in the creation of undesired signals.

Since they are located at different places in relation to the noise or crosstalk sources if the two wires are parallel, the impact of these unwanted signals is not the same in both cables (e,g., one is closer and the other is farther). This causes a change at the receiver. The pairings are twisted to maintain the equilibrium. For instance, let's say that in one twist, one wire is closer to the noise source than the other, and vice versa in the subsequent twist [6], [7].

Twisting increases the likelihood that both wires will be equally impacted by outside forces (noise or crosstalk). This indicates that no unwanted signals are received by the receiver, which computes the difference between the two. Most of the undesirable signals are eliminated. It is evident from the discussion above that the quality of the cable is somewhat influenced by the number of twists per length (for example, inch). Unshielded twisted-pair is the name given to the most popular kind of twisted-pair cable used in communications (UTP). Shielded twisted-pair is a kind of twisted-pair cable that IBM has created for its usage (STP). With STP cable, each pair of insulated conductors is covered by a metal foil or braided mesh. Metal casing increases cable quality by preventing noise or crosstalk from entering, but it is larger and more costly.

RJ45, or registered jack, is the most typical UTP connection. The RJ45 is a keyed connection, which means there is only one method to enter the connector. Telephone lines employ twisted-pair wires to provide voice and data channels. Unshielded twisted-pair cables are often used for the local loop, the connection connecting customers to the central telephone office. Unshielded twisted-pair cables' high bandwidth capabilities are also employed in the DSL lines that telephone companies use to provide high-data-rate connections. Since the two media are built quite differently, coaxial cable (also known as coax) can carry signals across greater frequency ranges than twisted-pair cable. Coax contains a central core conductor made of solid or stranded wire (often copper) that is coated in an insulating sheath, which is then covered by an exterior conductor made of metal foil, braid, or a mix of the two. The metallic covering on the outside functions as the circuit's second conductor as well as a noise-insulating barrier.

The whole cable is shielded by a plastic cover, and the exterior conductor is likewise covered in an insulating sheath. According to their radio government (RG) ratings, coaxial cables are classed. The wire gauge of the inner conductor, the thickness and type of the inner insulator, the design of the shield, and the size and type of the outer casing are all physical characteristics that are distinct to each RG number. Each cable with an RG classification is customized for a particular use. Coaxial connectors are required to connect coaxial cable to devices. The Bayone-Neill-Concelman (BNe) connection is the most often used kind of connector today.

The BNC connection, the BNC T connector, and the BNC terminator are three examples of these connectors that are widely used. The BNC connection is used to attach the cable's end to a gadget, such a TV. In Ethernet networks the BNC T connector is used to branch out to a connection to a computer or other device. At the end of the cable, a BNC terminator is utilised to stop signal reflection. In analogue telephone networks, coaxial cable was often utilised, and one coaxial network could transmit 10,000 voice transmissions. Subsequently, it was used in digital

telephone networks, allowing for the transmission of up to 600 Mbps of digital data over a single coaxial cable. Nonetheless, fiber-optic cable has essentially taken the role of coaxial wire in telephone networks today. Coaxial cables are also used by cable TV networks cable was utilised across the whole conventional cable TV network. The majority of the media, however, was later replaced by fiber-optic cable by cable TV providers; hybrid networks only employ coaxial cable at the network's edges, close to the customer premises. Coaxial cable RG-59 is used for cable TV.

Coaxial cable is also often used in conventional Ethernet LANs. Coaxial cable was used for digital transmission in the first Ethernet local area networks due to its large bandwidth and therefore fast data rate. The 10Base-2, also known as Thin Ethernet, transmits data at 10 Mbps across an 185 m-long distance using RG-58 coaxial cable with BNe connectors. The lOBase5, or Thick Ethernet, has a range of 5000 metres and transmits data at 10 Mbps using RG-11 thick coaxial cable. There are specific connections for thick Ethernet.

A fiber-optic cable transfers data as light and is composed of glass or plastic. We must first examine a number of facets of the nature of light in order to comprehend optical fiber. So long as it is travelling through a single homogeneous material, light moves in a straight path. A light ray's direction changes if it abruptly passes through one material and enters another with a different density. As seen in the image, the ray refracts and gets closer to the surface if the angle of incidence the angle the ray forms with the line perpendicular to the interface between the two substances is smaller than the critical angle. The light bends along the contact if the angle of incidence is equal to the critical angle. The beam reflects (turns) and passes once again through the denser material if the angle is larger than the critical angle. Remember that the critical angle is a characteristic of the substance and that different substances have different values for it.

Reflection is used by optical fibres to direct light through a channel. A less dense glass or plastic veneer surrounds a glass or plastic core. The two materials' different densities must be sufficiently different for a beam of light passing through the core to bounce off the cladding rather than be refracted into it. Multimode Since numerous beams from a single light source go through the core in various directions, multimode is so termed [8]. The density of the core in multimode step-index fibre is constant from the centre to the edges. Until it reaches the interface between the core and the cladding, a beam of light continues through this constant density in a straight line. A reduced density at the contact causes a sudden shift that changes the motion angle of the beam. The abruptness of this transition, which adds to the signal's distortion as it travels through the fibre, is referred to as the step index.

Multimode graded-index fibre, a different form of fibre, reduces this distortion of the signal travelling through the cable. The index of refraction is meant by the term "index" in this context. The index of refraction and density are connected, as we saw previously. Hence, a fibre with a graded index has different densities. The density of the core is strongest in the middle and progressively declines to its lowest point at the outside.

Using step-index fibre and a laser that is very concentrated, single-mode beams are restricted to a tiny range of angles that are all nearly horizontal. Singlemode fibre is produced with a much lower density and a considerably smaller diameter than multimode fibre (index of refraction). The critical angle is reduced as density decreases, and eventually approaches 90°, making beam propagation almost horizontal. The propagation of the various beams in this scenario is essentially similar, thus delays are minimal. The signal may be merged again with low signal

distortion even after all the beams arrive at the target "together." Electromagnetic waves are transported through unguided medium without the use of a physical conductor.

Wireless communication is a common name for this kind of communication. Signals are often transmitted via open space, making them accessible to anybody with a device that can pick them up. Unguided signals may go from their source to their destination in a number of modes, including line-of-sight, sky, and ground propagation. Radio waves hug the earth during ground propagation as they pass through the lowest layer of the atmosphere. From the transmitting antenna, these low-frequency waves radiate in all directions and follow the inclination of the earth. The stronger the signal, the larger the distance, which is dependent on signal power. Higher-frequency radio waves go upward during sky propagation into the ionosphere, where they are reflected back to earth by ions in that layer of the atmosphere. Using this transmission method, longer distances are possible with less output power.

Very high-frequency signals are carried from antenna to antenna in a straight line during line-of-sight propagation. Antennas need to be directed, facing one another, and although there isn't a definite line that separates radio waves from microwaves, electromagnetic waves with frequencies between 3 kHz and 1 GHz are often referred to as radio waves, while those with frequencies between 1 and 300 GHz are referred to as microwaves. Yet, a better categorization criteria is the way the waves behave rather than their frequency. Most of the time, radio waves are omnidirectional. Radio waves spread out in all directions when they are sent by an antenna. Hence, it is not necessary to align the transmitting and receiving antennas. Every receiving antenna may pick up the waves that a transmitting antenna transmits. Moreover, the omnidirectional characteristic has a drawback. A second antenna that may broadcast signals utilising the same frequency or band might interfere with the radio waves being sent by one antenna.

Radio waves may travel great distances, especially those that propagate in the sky mode. As a result, radio waves are an excellent choice for long-distance transmission, like AM radio. Walls may be penetrated by radio waves, especially those with low and medium frequencies. This trait has the potential to be both beneficial and harmful. It is helpful because, for instance, an AM radio may pick up signals within a structure. Since we cannot limit a conversation to only inside or outside a structure, this is a drawback. Compared to the microwave band, the radio wave band is comparatively small just under 1 GHz. This band's sub bands are likewise small, resulting in a poor data rate for digital communications when this band is broken into sub bands.

Authorities such as the FCC in the United States control almost the whole band. The authorities' approval is required before using any of the band antenna that is omnidirectional antennas are used by radio waves to broadcast signals anywhere. Radio waves are advantageous for multicasting because they are omnidirectional and have one transmitter but many receivers. Multicasting includes, but is not limited to, AM and FM radio, television, marine radio, cordless phones, and paging. Microwaves are electromagnetic waves with frequency between 1 and 300 GHz. Microwaves have just one direction. Microwave waves may be precisely focused when they are sent by an antenna. Hence, it is necessary to align the transmitting and receiving antennas. Unambiguously, the unidirectional attribute offers benefits. An antenna pair may be aligned without affecting another antenna pair that is already aligned. Some properties of microwave propagation are as follows:

Line-of-sight propagation applies to microwaves. Towers that are located far apart must be very tall because the towers with the attached antennas must be in close proximity to one another. Two short towers can't communicate with each other using microwaves due to the curvature of the earth and other obstructions. For long-distance communication, repeaters are often required. Walls cannot be penetrated by very high frequency microwaves[9], [10]. If receivers are located inside of structures, this trait may not be advantageous. The microwave band spans approximately 299 GHz, which is a broad range. As a result, broader sub-bands may be allocated, which allows for a greater data rate. Permission from authorities is required in order to use specific parts of the band.

Unidirectional antennas that transmit signals in a single direction are required for microwaves. For microwave communications, two kinds of antennas are used: the parabolic dish and the homing. A parabola's geometry serves as the foundation for a parabolic dish antenna. Every line that is perpendicular to the line of symmetry the line of sight reflects off the curve at different angles, resulting in an intersection of all the lines known as the focus.

CONCLUSION

Transmission media play a critical role in the effectiveness of communication systems. Guided media, such as twisted pair cable, coaxial cable, and fiber optic cable, are commonly used for transmitting signals in LANs and WANs, while unguided media, such as radio waves, microwaves, and infrared waves, are used for wireless communication. Each type of transmission medium has its own advantages and disadvantages, and several factors must be considered when selecting a medium, including bandwidth, distance, interference, cost, and reliability.

REFERENCES

[1] K. Nakajima, P. Sillard, D. Richardson, M. J. Li, R. J. Essiambre, and S. Matsuo, “Transmission media for an SDM-based optical communication system,” *IEEE Commun. Mag.*, 2015, doi: 10.1109/MCOM.2015.7045390.

[2] O. Schierz, H. Müller, C. S. Stingu, S. Hahnel, and A. Rauch, “Dental tray adhesives and their role as potential transmission medium for microorganisms,” *Clin. Exp. Dent. Res.*, 2021, doi: 10.1002/cre2.432.

[3] W. Bu, G. Shen, H. Qiu, and C. Liu, “Investigation on the dynamic influence of thermophysical properties of transmission medium on the internal flow field for hydraulic retarder,” *Int. J. Heat Mass Transf.*, 2018, doi: 10.1016/j.ijheatmasstransfer.2018.05.037.

[4] S. Bi, C. Wang, Z. Yuan, J. Zhu, W. W. Xu, and Y. Yu, “Influence of the transmission medium on the focusing performance of gradient-index fiber probe,” *Optik (Stuttg).*, 2016, doi: 10.1016/j.ijleo.2015.12.082.

[5] N. Cho, J. Yoo, S. J. Song, J. Lee, S. Jeon, and H. J. Yoo, “The human body characteristics as a signal transmission medium for intrabody communication,” *IEEE Trans. Microw. Theory Tech.*, 2007, doi: 10.1109/TMTT.2007.895640.

[6] R. Róka and M. Mokráň, “Modeling of the PSK utilization at the signal transmission in the optical transmission medium,” *Int. J. Commun. Networks Inf. Secur.*, 2015, doi: 10.17762/ijcnis.v7i3.1471.

[7] J. H. Fu *et al.*, “Liquid metal hydraulics paradigm: Transmission medium and actuation of bimodal signals,” *Sci. China Technol. Sci.*, 2022, doi: 10.1007/s11431-021-1900-x.

[8] R. Róka and F. čertík, “Modeling of environmental influences at the signal transmission in the optical transmission medium,” *Int. J. Commun. Networks Inf. Secur.*, 2012, doi: 10.17762/ijcnis.v4i3.233.

[9] V. P. Kvasnikov, S. V. Yehorov, T. Y. Shkvarnytska, D. P. Ornatskyi, and M. A. Kataieva, “Modeling Communication Systems To Study The Effect Of Interference In The Transmission Medium,”*Radio Electron. Comput. Sci. Control*, 2022, doi: 10.15588/1607-3274-2021-4-2.

[10] C. Thornton, “Force transmission in granular media,” *KONA Powder and Particle Journal*. 1997. doi: 10.14356/kona.1997012.

CHAPTER 13

SWITCHING: A REVIEW OF CIRCUIT, PACKET, AND MESSAGE SWITCHING TECHNIQUES FOR EFFICIENT AND SCALABLE DATA COMMUNICATION NETWORKS

Rahul Vishnoi, Assistant Professor
Department of Electronics and Communication Engineering, Teerthanker Mahaveer University, Moradabad, Uttar Pradesh, India
Email Id- ra_v@yahoo.com

ABSTRACT:

Switching is a fundamental concept in computer networking that refers to the process of forwarding data packets between network devices. It is a critical component of communication systems that allows multiple devices to share a common transmission medium, such as a network cable or wireless link. There are several types of switching technologies, including circuit switching, packet switching, and message switching, each with its own unique characteristics and applications. Circuit switching involves establishing a dedicated physical connection between two network devices, enabling them to communicate without interference from other devices. It is commonly used in applications that require guaranteed bandwidth and low latency, such as voice and video communications. Packet switching, on the other hand, involves breaking data into small packets and forwarding them individually through the network. This allows multiple devices to share the same transmission medium and is commonly used in LANs and WANs. Message switching is a less common form of switching that involves forwarding entire messages between network devices.

KEYWORDS:

Bandwidth, Circuit, Switching, Local Area Network (LAN), Network Devices, Wide Area Network (WAN).

INTRODUCTION

Switching refers to the process of connecting different network devices together in order to enable data transmission between them. This involves directing data packets from one device to another through a switching network. Switching is an essential component of modern telecommunications networks, including both local area network(LAN) and wide area network (WAN) environments. In this article, we will discuss different types of switches, their functions, and how they are used in modern network architecture. There are three main types of switches: LAN, WAN, and MAN (metropolitan area network) switches. Each of these types of switches performs a specific function within the network infrastructure.

LAN switches are the most common type of switches and are used to connect devices within a local area network. These switches operate at Layer 2 of the OSI model, which means that they use MAC (media access control) addresses to direct data packets from one device to another. LAN switches can be further categorized as unmanaged, managed, and smart switches [1], [2]. Unmanaged switches are the simplest type of switch and require no configuration. They are

plug-and-play devices that can be used to connect devices within a LAN. Unmanaged switches typically have a fixed number of ports and are ideal for small networks. Managed switches are more complex than unmanaged switches and offer more control over network traffic. They can be configured to prioritize traffic and manage network security. Managed switches are typically used in larger networks that require more control over network traffic [3], [4]. Smart switches are a hybrid between unmanaged and managed switches. They offer some degree of control over network traffic but do not have the advanced features of a fully managed switch. Smart switches are ideal for small to medium-sized networks. WAN switches are used to connect devices over a wide area network. These switches operate at Layer 3 of the OSI model, which means that they use IP addresses to direct data packets from one device to another. WAN switches can be further categorized as routers and layer 3 switches.

Routers are the most common type of WAN switch and are used to connect devices across different networks. They direct data packets between different networks using IP addresses. Routers can be further categorized as edge routers and core routers. Edge routers are used to connect devices at the edge of the network, while core routers are used to route traffic within the network. Layer 3 switches are a hybrid between routers and LAN switches. They offer some of the routing functionality of a router and the switching functionality of a LAN switch. Layer 3 switches are typically used in medium-sized networks that require more control over network traffic. MAN switches are used to connect devices within a metropolitan area network. These switches operate at Layer 2 of the OSI model, which means that they use MAC addresses to direct data packets from one device to another. MAN switches are typically used in large cities where a single LAN is too small to handle the volume of network traffic.

Switches perform several key functions in network infrastructure. The primary function of a switch is to direct data packets from one device to another. When a data packet is received by a switch, the switch reads the destination MAC or IP address and sends the packet to the appropriate device. This process is known as packet forwarding. Switches also manage network traffic by prioritizing certain types of traffic. For example, in a VoIP (voice over IP) network, voice traffic is given a higher priority than other types of traffic. This ensures that voice calls are not disrupted by other types of network traffic [5].

Switches also improve network security by separating different segments of a network. This is done by creating VLANs (virtual LANs), which are logical groups of devices that are separated from other groups. VLANs improve security by isolating different segments of a network and preventing unauthorized access. Improve network performance by using techniques such as load balancing and link aggregation. Load balancing involves distributing network traffic evenly across multiple links. This ensures that no single link becomes overloaded and helps to prevent network congestion. Link aggregation involves combining multiple links into a single logical link. This increases the bandwidth available for network traffic and provides redundancy in case one link fails.

DISCUSSION

There are several switching technologies that are commonly used in modern networks. The two main types of switches are LAN switches and WAN switches. LAN switches are used to connect devices within a LAN, while WAN switches are used to connect devices over a wide area network. LAN switches are used to connect devices within a LAN. LAN switches use the Media Access Control (MAC) address of each device to forward packets. MAC addresses are unique

identifiers assigned to each network interface controller (NIC) of a device. When a device sends a packet, the LAN switch checks the destination MAC address of the packet and forwards the packet to the correct port [6] .

There are several types of LAN switches, including unmanaged switches, managed switches, and Layer 3 switches. Unmanaged switches are simple switches that have no configuration options. They are typically used in small networks with a few devices. Managed switches are more complex switches that can be configured using a CLI or GUI. They are typically used in medium to large networks. Layer 3 switches are switches that can perform routing functions in addition to switching functions. They can be used to connect different VLANs within a network.

WAN switches are used to connect devices over a wide area network. WAN switches use routing tables to forward packets. Routing tables contain information about the network topology and the best path to reach a destination network. When a packet is received, the WAN switch checks the destination IP address of the packet and consults the routing table to determine the best path to forward the packet. There are several types of WAN switches, including routers, Layer 3 switches, and ATM switches. Routers are devices that are used to connect different networks together. They use routing tables to forward packets between networks. Layer 3 switches can perform routing functions in addition to switching functions. They can be used to connect different VLANs within a network. ATM switches are used to transmit data over an Asynchronous Transfer Mode (ATM) network. ATM is a high-speed networking technology that is used for data, voice, and video transmission.

Switches use several techniques to improve network performance and security. These techniques include VLANs, load balancing, link aggregation, and Quality of Service (QoS). VLANs are virtual LANs that are used to logically segment a network. VLANs allow network administrators to create separate broadcast domains within a single physical network. Devices within a VLAN can communicate with each other, but they cannot communicate with devices in other VLANs. VLANs can be used to improve network performance and security by reducing network congestion and preventing unauthorized access to sensitive network resources.

Load balancing is a technique that is used to distribute network traffic evenly across multiple links. Load balancing helps to prevent network congestion by ensuring that no single link becomes overloaded. Load balancing can be performed at the switch level or at the router level. Switch-level load balancing is performed by distributing traffic across multiple ports on a single switch. Router-level load balancing is performed by distributing traffic across multiple routers.Link aggregation is a technique that is used to combine multiple links into a single logical link. Link aggregation increases the bandwidth available for network traffic and provides redundancy in case one link fails. Link aggregation can be performed using several protocols, including Link Aggregation Control Protocol (LACP) and Port Aggregation Protocol (PAgP).

Quality of Service (QoS) is a technique that is used to prioritize network traffic based on its importance. QoS can be used to ensure that high-priority traffic, such as voice and video, is given priority over low-priority traffic, such as email and web browsing. QoS is typically implemented at the switch or router level and uses different techniques, switches can also provide monitoring and management capabilities. Managed switches can be configured using a command-line interface (CLI) or a graphical user interface (GUI). This allows network administrators to monitor network traffic, configure network settings, and troubleshoot network issues [7].

In modern network architecture, switching plays a critical role in the functioning of the network. LAN switches are used to connect devices within a LAN, while WAN switches are used to connect devices over a wide area network. The use of VLANs, load balancing, and link aggregation techniques help to improve network performance and security. Switching also plays a key role in the development of cloud computing and virtualization technologies. Virtual switches are used to connect virtual machines (VMs) within a virtualized environment. This allows multiple VMs to communicate with each other and with physical devices on the network.

Virtual switches can be managed using the same tools as physical switches, allowing network administrators to manage both physical and virtual switches from a single interface. Another emerging technology in network architecture is software-defined networking (SDN). SDN separates the control plane and data plane of the network, allowing network administrators to centrally manage the network. SDN uses a centralized controller to manage network traffic and configure network settings. SDN switches are used to direct network traffic based on instructions from the controller.

A group of interconnected devices form a network. The challenge of connecting several devices to enable one-to-one communication arises whenever we have a number of them. Making a point-to-point link (a mesh) between each pair of devices is one option between a core device and every other device (topology) (a star topology). When used on extremely large networks, these techniques are inefficient and wasteful [8]. In order to be cost-effective, the quantity and length of the linkages need too much infrastructure, and the bulk of those lines would remain idle the majority of the time. Alternative multipoint topologies, such a bus, are disqualified since the number of devices and the distances between them exceed the capabilities of the medium and hardware. A switched network is made up of several interconnected nodes, or switches. Switches are tools that enable momentary connections between two or more connected devices. Some of these nodes are linked to the end systems in a switched network (computers or telephones, for example). Some are just used for routing. Circuit switching, packet switching, and message switching have historically been three crucial switching techniques. Nowadays, the first two are often used. While the third has been phased away in regular communications, networking still uses it.

The three major types of today's networks are circuit-switched, packet-switched, and message-switched. Virtual-circuit networks and datagram networks are the two additional subcategories that may be used to separate packet-switched networks. We may claim that virtual-circuit networks and circuit-switched and datagram networks share certain traits. As a result, we start by talking about circuit-switched networks before moving on to datagram networks and eventually virtual-circuit networks. In packet switching nowadays, it is common to mix datagram networks with virtual circuit networks. The initial packet is routed by networks using the concept of datagram addressing, but the subsequent packets that originate from the same source and go to the same destination are routed using a virtual-circuit network. Several of these networks will be shown to us in next chapters. Each switch in message switching saves the whole message before forwarding it to the next switch. Despite the fact that message switching is not visible at lower levels, it is nonetheless used in certain applications, such as email (e-mail). This subject will not be covered in this book. A network with circuit switching comprises of switches that are physically linked together.A dedicated route composed of one or more connections is referred to as a connection between two stations. For each link, however, there is only one dedicated channel used by each connection. Typically, each connection is split into n channels using FDM

or TDM. Although while multiplexing might be implicitly incorporated in the switch fabric, we have clearly displayed the multiplexing symbols to underline the split of the connection into channels.

The switch is directly linked to the end systems, such as computers or phones. For sake of simplicity, we have simply shown two end systems. When end system A and end system M need to interact, end system A must request a connection to M, which must be approved by all switches in addition to M. The setup step is when each connection reserves a circuit (channel), and the mix of circuits or channels determines the dedicated route. Data transmission is possible after the dedicated route, which consists of linked circuits (channels), has been created. The circuits are shut off when all the data has been transmitted.

The stations must reserve the resources they will need throughout the conversation before the communication can begin. Channels (bandwidth in FDM and time slots in TDM), switch buffers, switch processing time, and switch input/output ports must all be devoted throughout the data transmission process until the takedown stage [9] . Physical layer signal communication between the two stations does not use packetized data. Notwithstanding any silent intervals, the data are transferred continuously from the source station to the destination station. Data transport does not include any addressing.

The switches direct the data according to the time slot or band that is occupied (FDM) (TDM). Naturally, end-to-end addressing is employed throughout the setup stage, as we shall see in a moment. Three stages are necessary for the actual communication in a circuit-switched network: connection establishment, data transmission, and connection deconstruction.

A dedicated circuit (combination of channels in connections) must be created prior to communication between the two parties (or numerous parties participating in a conference call). Connection configuration entails setting up dedicated channels between the switches as the end systems are often linked to them through dedicated lines. For instance, when system A wants to connect to system M, switch I receives a setup request from system that contains system M's address. Switch I locates a channel that may be set aside for this purpose between itself and switch IV. The request is then sent from switch I to switch IV, which establishes a dedicated channel between switch IV and switch III. System M is being informed of system A's purpose through Switch III.

The next stage in establishing a link is for system M to acknowledge system A in the other way. The link is not established until system A gets this acknowledgement. Be aware that establishing a link between the two end systems requires end-to-end addressing. They may, for instance, be phone numbers in an FDM network or the administrator-assigned computer addresses in a TDM network. The two parties may transmit data after creating the specialized circuit (channels). A signal to release the resources is delivered to each switch when one of the parties has to disconnect.

Since resources are provided for the lifetime of the connection, it might be claimed that circuit-switched networks are less effective than the other two kinds of networks. Other connections are unable to access these resources. On a telephone network, conversations often come to an end after both parties have completed speaking. In contrast, a computer may still be linked to another computer in a network even if there has been a lengthy period of inactivity. In this situation, permitting resources to be allocated results in the deprivation of other connections. Despite the

fact that a circuit-switched network often has poor efficiency, its delay is quite small. Resources are allotted for the lifetime of the connection during data transmission; data are not delayed at each transition [10].

The time required to establish the connection, send the data, and close the circuit accounts for the whole delay. The propagation time of the source computer's request (first grey box's slope), the request signal transfer time (first grey box's height), the propagation time of the destination computer's acknowledgment (second grey box's slope), and the signal transfer time of the acknowledgment together make up the setup's total delay (height of the second grey box). The propagation time (shown by the slope of the colored box) and data transmission time (represented by the height of the colored box), both of which may be quite lengthy, together make up the delay caused by data transfer. The third box displays how long it will take to disassemble the circuit. The scenario that results in the greatest delay has been shown. The receiver wishes to be disconnected. The telephone companies traditionally picked the circuit-switched method to switching at the physical layer, but the trend now is shifting towards other switching approaches. For instance, the phone number is utilized as the global address, and the setup and takedown processes employ asignaling system.

CONCLUSION

Switching is a fundamental concept in networking that involves the movement of data packets from one network device to another. Switches are essential components in both local area networks (LANs) and wide area networks (WANs) and are used to connect devices and networks together. There are several types of switches, including LAN switches, WAN switches, and hybrid switches that combine the functionality of both types [11] . Switches use various techniques to improve network performance and security, such as VLANs, load balancing, link aggregation, and Quality of Service (QoS). VLANs allow network administrators to logically segment a network and improve network security by limiting communication between devices in different VLANs. Load balancing helps to prevent network congestion by distributing network traffic evenly across multiple links. Link aggregation combines multiple links into a single logical link to increase available bandwidth and provide redundancy. QoS prioritizes network traffic based on its importance and helps to ensure that high-priority traffic is given priority over low-priority traffic

REFERENCES

[1] M. J. Wheelock, Y. Shintani, M. Maeda, Y. Fukumoto, and K. R. Johnson, “Cadherin switching,” *Journal of Cell Science*. 2008. doi: 10.1242/jcs.000455.

[2] F. Schmitz and A. Voss, “Components of task switching: A closer look at task switching and cue switching,” *Acta Psychol. (Amst).*, 2014, doi: 10.1016/j.actpsy.2014.06.009.

[3] Y. Q. Yusuf, I. A. Fata, and Chyntia, “Types of Indonesian-English code-switching employed in a novel,” *Kasetsart J. Soc. Sci.*, 2020, doi: 10.1016/j.kjss.2018.02.004.

[4] S. Siegel *et al.*, “Trade-Off Between Data Retention and Switching Speed in Resistive Switching ReRAM Devices,” *Adv. Electron. Mater.*, 2021, doi: 10.1002/aelm.202000815.

[5] S. Y. Youn, J. E. Lee, and J. Ha-Brookshire, “Fashion Consumers’ Channel Switching Behavior During the COVID-19: Protection Motivation Theory in the Extended Planned Behavior Framework,” *Cloth. Text. Res. J.*, 2021, doi: 10.1177/0887302X20986521.

[6] M. Timmermeister, P. Leseman, F. Wijnen, and E. Blom, "No Bilingual Benefits Despite Relations Between Language Switching and Task Switching," *Front. Psychol.*, 2020, doi: 10.3389/fpsyg.2020.01832.

[7] S. Monsell, "Task switching," *Trends in Cognitive Sciences*. 2003. doi: 10.1016/S1364-6613(03)00028-7.

[8] G. Wen, X. Yu, W. Yu, and J. Lu, "Coordination and Control of Complex Network Systems with Switching Topologies: A Survey," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*. 2021. doi: 10.1109/TSMC.2019.2961753.

[9] C. B. Saper, P. M. Fuller, N. P. Pedersen, J. Lu, and T. E. Scammell, "Sleep State Switching," *Neuron*. 2010. doi: 10.1016/j.neuron.2010.11.032.

[10] M. Deuchar, "Code-switching in linguistics: A position paper," *Languages*, 2020, doi: 10.3390/languages5020022.

[11] E. Bosma and E. Blom, "A code-switching asymmetry in bilingual children: Code-switching from Dutch to Frisian requires more cognitive control than code-switching from Frisian to Dutch," *Int. J. Biling.*, 2019, doi: 10.1177/1367006918798972.

CHAPTER 14

DATAGRAM NETWORKS: AN ANALYSIS OF DATAGRAM PACKET SWITCHING TECHNIQUES FOR RELIABLE AND EFFICIENT DATA COMMUNICATION

Pankaj Kumar Goswami, Associate Professor
Department of Electronics and Communication Engineering, Teerthanker Mahaveer University, Moradabad, Uttar Pradesh, India
Email Id- g.pankaj1@gmail.com

ABSTRACT:

Datagram networks are a type of computer network where data is transmitted in discrete units known as datagrams. These datagrams are individually addressed and routed through the network independently of one another, allowing for more flexible and efficient data transmission compared to other types of networks. In a datagram network, each data packet, or datagram, contains a destination address and source address, as well as the data to be transmitted. The network uses this information to determine the best route for the datagram to take to reach its destination. This approach allows for more efficient use of network resources since the network can dynamically adjust its routing decisions based on network conditions and traffic.

KEYWORDS:

Datagram, Data Transmission, Internet Protocol, Network, Traffic.

INTRODUCTION

Datagram networks are commonly used in the Internet, where they form the basis of the Internet Protocol (IP) network layer. In this layer, datagrams are used to transmit data across the network, and IP addresses are used to identify the source and destination of each datagram. Because datagrams are transmitted independently of one another, the IP protocol can provide a highly flexible and adaptable network infrastructure. Datagram networks are often contrasted with circuit-switched networks, which establish a dedicated connection between two endpoints for the duration of a data transmission. Circuit-switched networks are highly reliable, but they are also inflexible and can be inefficient when used for data transmissions that do not require a continuous connection [1], [2].

One of the key advantages of datagram networks is their flexibility and scalability. Because datagrams are transmitted independently of one another, datagram networks can handle a wide variety of data types and network topologies. This makes them well-suited for applications that require a high degree of flexibility and adaptability, such as the Internet of Things (IoT) and real-time communications. Another advantage of datagram networks is their ability to dynamically adjust their routing decisions based on network conditions and traffic. This can help to ensure that data is transmitted quickly and efficiently, even in the face of network congestion or other disruptions. In addition, because datagrams can be transmitted in any order, datagram networks can provide a high degree of fault tolerance and redundancy[3] .

However, the connectionless and best-effort nature of datagram networks can also introduce some challenges. Because there is no guaranteed delivery or reliability, applications that require high levels of data integrity and security may need to implement additional measures to ensure data is transmitted and received correctly. Additionally, the lack of a dedicated connection for each data transmission can result in higher levels of network congestion and lower network performance in high-traffic situations. One way to address these challenges is to implement protocols that provide additional functionality on top of the basic datagram network. For example, the Transmission Control Protocol (TCP) provides a reliable, connection-oriented data transmission service that can be used to ensure data integrity and security. By establishing a dedicated connection between two endpoints and using a sequence of numbered packets, TCP can help to ensure that data is transmitted and received correctly [4], [5].

Another way to improve the performance and reliability of datagram networks is to implement Quality of Service (QoS) measures. QoS allows network administrators to prioritize certain types of data traffic over others, which can help to ensure that high-priority traffic is given priority over lower-priority traffic. This can be particularly useful for real-time applications, such as video and voice communications, which require low latency and high throughput. In addition to these protocols and measures, there are also several techniques and technologies that can be used to improve the performance and reliability of datagram networks. These include:

1. **Load balancing:** Load balancing distributes network traffic evenly across multiple links, which can help to prevent network congestion and improve overall network performance.
2. **Link aggregation:** Link aggregation combines multiple links into a single logical link, which can increase available bandwidth and provide redundancy in case of a link failure.
3. **Virtual Local Area Networks (VLANs):** VLANs allow network administrators to logically segment a network and improve network security by limiting communication between devices in different VLANs.
4. **Multiprotocol Label Switching (MPLS):** MPLS is a protocol that uses labels to route data packets through a network, allowing for more efficient use of network resources and faster data transmission.
5. **Network Address Translation (NAT):** NAT is a technique used to map one IP address space into another by modifying network address information in the IP header of packets while they are in transit across a traffic routing device.
6. **Firewalls:** Firewalls are network security devices that monitor and control incoming and outgoing network traffic, based on predetermined security rules.
7. **Virtual Private Networks (VPNs):** VPNs provide a secure and encrypted connection over the Internet, allowing remote users to access a private network as if they were directly connected to it.

Datagram networks provide a flexible and efficient network infrastructure that can handle a wide variety of data types and network topologies. By implementing additional protocols and measures, as well as using advanced techniques and technologies, it is possible to address many of the challenges associated with datagram networks and improve their performance, reliability, and security.

DISCUSSION

One of the key features of datagram networks is their ability to handle a wide variety of data types and applications. For example, datagram networks are commonly used for streaming video and audio, online gaming, and real-time communications such as VoIP (Voice over Internet Protocol). Because datagram networks are connectionless and best-effort, they can provide low-latency and high-throughput data transmission, which is essential for these types of applications.

However, the connectionless nature of datagram networks can also introduce some security challenges. Because there is no guaranteed delivery or reliability, it is possible for attackers to intercept or modify data packets as they are transmitted across the network. To address these security concerns, various security measures have been developed, such as the use of encryption and digital signatures to protect data packets, and firewalls to filter incoming and outgoing network traffic. Another advantage of datagram networks is their ability to scale up or down as needed. Because datagram networks are inherently distributed, it is possible to add or remove nodes from the network without disrupting overall network performance. This scalability is essential for large-scale applications such as cloud computing, where data centers must be able to handle rapidly changing workloads and traffic patterns.

In addition, datagram networks are often used in conjunction with other types of networks, such as local area networks (LANs) and wide area networks (WANs). By connecting multiple networks together, it is possible to create a seamless and integrated network infrastructure that can handle a wide range of applications and services. We must transmit messages from one end system to another in data communications. The message must be broken into packets of a fixed or variable size if it is to go across a packet-switched network. The network and the controlling protocol decide the packet's size [6] . There is no resource allocation for a packet in packet switching. As a result, there is no planned processing time for each packet and no allocated capacity on the networks. On demand allocation of resources occurs. First-come, first-served policy governs the distribution of resources. No matter the source or destination of a packet when it is received by a switch, it must wait if another packet is already being processed. This lack of reservation might cause delays, much like other systems in our everyday lives. For instance, if we don't have a reservation at a restaurant, each packet in a datagram network is handled separately from every other packet. The network handles each packet as if it were an independent entity, even if it were a part of a multipacket transfer. In this method, packets are known as datagrams.

The network layer is often where datagram switching takes place. Here, we compare datagram networks to circuit-switched and virtual-circuit-switched networks in a concise manner. In this text's fourth and last part, we delve into further depth. Four packets are sent from station A to station X using the datagram technique. In a datagram network, switches are often referred to as routers. The four packets (or datagrams) in the illustration all belong to the same message but may take various routes to get there, which is why we've used a separate symbol for the switches. This is true because the connections could also be transporting packets from other sources and hence might not have enough capacity to send all of the packets from A to X. This method may result in differing delays between the packets of a transmission, causing the datagrams to arrive at their destination out of order. Moreover, a shortage of resources may cause packets to be dropped or lost. In most protocols, an upper-layer protocol is in charge of reordering the datagrams or requesting missing datagrams before handing them off to the application.

The term "connectionless networks" is occasionally used to describe datagram networks. The term "connectionless" in this context refers to the fact that the switch (packet switch) does not maintain connection status data. There are no phases for setup or breakdown. A switch treats every packet equally regardless of its source or destination [7], [8]. How are the packets routed to their destinations in a datagram network if there are no setup or teardown phases? Each switch (or packet switch) in this kind of network has a routing table that is based on the destination address. Routing tables are dynamic and are often updated. The tables include the destination addresses and the appropriate forwarding output ports. This contrasts with a circuit-switched network's table, where each item is added after the setup step is finished and removed when the takedown phase is finished.

Each packet in a datagram network has a header that includes, among other things, the packet's destination address. This destination address is evaluated when the packet is received by the switch, and the routing table is used to determine the appropriate port via which the packet should be sent. This address stays the same during the whole travel of the packet, unlike the address in a virtual-circuit-switched network. A datagram network is more efficient than a circuit-switched network since resources are only allocated when packets need to be sent. Resources may be redistributed during these minutes for other packets from other sources if a source transmits a packet and there is a wait of a few minutes before another packet can be delivered. A datagram network may have more latency than a virtual-circuit network. Each packet could wait at a switch before being transmitted, even if there are no setup and teardown steps. Also, the delay is not constant across all of the packets in a message since not all of them must pass through the same switches. A virtual-circuit network is a hybrid of a datagram network and a circuit-switched network.

Switches in the network enable traffic from sources to destinations. Computers, packet switches, bridges, and other networking equipment may all serve as sources or destinations. There are two different addressing types used in virtual-circuit networks: global and local (virtual-circuit identifier). A source or destination must have a global address; this address might be exclusive to the network or, if the network is a component of a global network, to the whole world. But, as we shall see in the discussion that follows, a global address in virtual-circuit networks is only utilised to generate a virtual-circuit identification.

The virtual-circuit identification is the name of the identifier that is actually used for data transmission (Vel). A frame between two switches uses a vel, a tiny number with switch-only scope as opposed to a global address. A frame has a VCI when it enters a switch, and a different VCl when it exits. The VCI in a data frame transitions from one switch to another. It should be noted that a VCI does not necessarily need to be a big number since each switch might employ a different set of VCls.A source and destination in a virtual-circuit network must go through three stages, similar to those in a circuit-switched network: setup, data transmission, and teardown. During setup, switches create connection-specific table entries with the help of the source and destination's global addresses. The source and destination instruct the switches to remove the matching entry during teardown. Between these two periods, data transmission takes place. We start with the simpler data transmission step and go on to the more complex setup and takedown stages.

Every switches need to have a table entry for this virtual circuit in order to move a frame from a source to its destination. The table comprises four columns in its most basic form. Thus, the

switch stores four bits of data for every virtual circuit that has previously been established. In the meanwhile, we assume that each switch has a table with entries for all active virtual circuits. We will demonstrate how the switches produce their table entries later. Until the source transfers all of its frames to the destination, the data transmission phase is active. Each frame of a message is processed in the same way at the switch. Between the source and the destination, the procedure establishes a virtual circuit rather than a physical one. A switch produces an entry for a virtual circuit during setup. Assume, for instance, that source a needs to build a virtual circuit to source B. The setup request and the acknowledgment are both necessary stages. The switch selects an available incoming VCI and assigns the incoming port together with the outgoing port. The outgoing VCI, which will be discovered during the acknowledgement stage, is not yet known to it. The switch then transmits the frame to switch 2 via port 3.

The setup request frame is received by Switch 2. Similar events occur at this location as they did at switch 1, and three columns of the table are filled up in this instance: incoming port, incoming VCI (66), and outgoing port. The setup request frame is received by Switch 3. Once again, the three columns for the incoming port, incoming VCI, and leaving port are finished. After Destination B has received the setup frame, if it is prepared to accept frames from A, it assigns a VCI, in this example 77, to the incoming frames from A. The destination is informed by this VCI that the frames originate from A and not from any other sources. Acknowledgment the switching tables' entries are finished by a unique frame known as the acknowledgement frame. Switch 3 receives an acknowledgement from the destination. The switch understands which item in the table has to be finished since the acknowledgement includes the global source and destination addresses. The destination selected VCI 77 as the incoming VCI for frames from A, and it is likewise carried in the frame. This VCI is used by Switch 3 to finish the entry's incoming VCI column. Notably, 77 is the outgoing VCI for switch 3, but the entering VCI for destination B.

Switch 3 notifies switch 2 that its incoming VCI is in the table that was previously selected. This serves as the outgoing VCI in the table for Switch 2. Switch 2 then notifies switch 1 of its incoming VCI in the table that was previously selected in step c. This serves as the incoming VCI for Switch 1 in the table. Switch 1 then notifies source A of the receipt of its incoming VCI in the table that was selected earlier. This is the outgoing VCI that the source uses to send the data frames to destination B. One important use case for datagram networks is in the Internet of Things (IoT) and machine-to-machine (M2M) communications. The growing number of connected devices and sensors in the IoT requires a network infrastructure that can handle large amounts of data traffic in a scalable and efficient manner. Datagram networks are well-suited for this task, as they can handle low-latency, high-throughput data transmission, and can be easily scaled up or down as needed.

Another important feature of datagram networks is their ability to support multicast communication. Multicast allows a single data packet to be sent to multiple recipients simultaneously, which can be more efficient than sending individual packets to each recipient separately. This is especially useful for applications such as video and audio streaming, where multiple users may be watching or listening to the same content simultaneously. In addition, datagram networks are used in many real-time applications such as financial trading, online gaming, and teleconferencing. These applications require low-latency and high-throughput data transmission, which is precisely what datagram networks are designed to provide. However, there are also some challenges associated with datagram networks. Because there is no guaranteed delivery or reliability, it is possible for data packets to be lost or delayed in

transmission. To address this issue, various protocols and techniques have been developed, such as packet loss detection and retransmission, congestion control, and flow control.

Another challenge with datagram networks is their vulnerability to network attacks such as Distributed Denial of Service (DDoS) attacks. Because datagram networks are connectionless, it is possible for attackers to flood the network with large numbers of packets, overwhelming the network and disrupting normal operations [9], [10]. To mitigate the risk of DDoS attacks, various measures can be implemented such as filtering incoming network traffic, limiting the number of requests per second, and implementing security protocols to protect against malicious traffic datagram networks are a flexible and efficient network infrastructure that can handle a wide variety of data types and applications. By using additional protocols and measures, it is possible to address many of the challenges associated with datagram networks and improve their performance, reliability, and security. As new applications and technologies emerge, it is likely that datagram networks will continue to play an important role in the development and deployment of innovative solutions.

CONCLUSION

Datagram networks are an important type of network infrastructure that are widely used in a variety of applications and industries. Their connectionless, best-effort approach to data transmission makes them well-suited for real-time applications such as streaming media and online gaming, as well as IOT and M2M communications. Datagram networks are also highly scalable, allowing for the addition or removal of nodes without disrupting overall network performance. As network technologies continue to evolve, it is likely that datagram networks will continue to play an important role in the development and deployment of new applications and services [11], [12]. By using advanced protocols and techniques, as well as implementing measures to improve their performance, reliability, and security, datagram networks can continue to provide a flexible and efficient network infrastructure for a wide range of applications and industries.

REFERENCES

[1] E. Aharoni and R. Cohen, “Restricted dynamic Steiner trees for scalable multicast in datagram networks,” *IEEE/ACM Trans. Netw.*, 1998, doi: 10.1109/90.700892.

[2] C. J. Bennett, A. J. Hinchley, and S. W. Edge, “Issues in the Interconnection of Datagram Networks,” *IEN 1 - INDRA Note 637*, 1977.

[3] E. Ekici, I. F. Akyildiz, and M. D. Bender, “A distributed routing algorithm for datagram traffic in LEO satellite networks,” *IEEE/ACM Trans. Netw.*, 2001, doi: 10.1109/90.917071.

[4] G. Di Caro and M. Dorigo, “AntNet: Distributed stigmergetic control for communications networks,” *J. Artif. Intell. Res.*, 1998, doi: 10.1613/jair.530.

[5] G. Di Caro and M. Dorigo, “Two ant colony algorithms for best-effort routing in datagram networks,” *Proc. Tenth IASTED Int. Conf. Parallel Distrib. Comput. Syst.*, 1998.

[6] J. B. Nagle, “On packet switches with infinite storage,” *IEEE Transactions on Communications*. 1987. doi: 10.1109/TCOM.1987.1096782.

[7] A. Demers, S. Keshav, and S. Shenker, “Analysis and simulation of a fair queueing algorithm,” *Comput. Commun. Rev.*, 1995, doi: 10.1145/75246.75248.

[8] C. Hornig, “A Standard for the Transmission of IP Datagrams over Ethernet Networks,” *Req. Comments*, 1984.

[9] J. H. Huh, “Reliable user datagram protocol as a solution to latencies in network games,” *Electron.*, 2018, doi: 10.3390/electronics7110295.

[10] W. L. Price, “SIMULATION STUDIES OF DATA COMMUNICATION NETWORKS OPERATING IN DATAGRAM MODE.,” *Comput. J.*, 1978, doi: 10.1093/ comjnl/ 21.3.219.

[11] J. Melorose, R. Perroy, and S. Careas, “Compression Format for IPv6 Datagrams over IEEE 802.15.4-Based Networks,” *Statew. Agric. L. Use Baseline 2015*, 2015.

[12] J. Mogul, “Broadcasting Internet datagrams in the presence of subnets,” *RFC 922, Netw. Work. Gr.*, 1984.

CHAPTER 15

USING TELEPHONE AND CABLE NETWORKS FOR DATA TRANSMISSION: A COMPARATIVE ANALYSIS OF DSL AND CABLE MODEM TECHNOLOGIES FOR HIGH-SPEED AND RELIABLE DATA COMMUNICATION

Rahul Sharma, Assistant Professor
Department of Electronics and Communication Engineering, Teerthanker Mahaveer University, Moradabad, Uttar Pradesh, India
Email Id- drrahuls.iitk@gmail.com

ABSTRACT:

Using telephone and cable networks for data transmission is a common practice in modern communication. With the advancements in technology, these networks have become faster and more reliable, making them a viable option for transmitting large amounts of data. This abstract provides an overview of the key concepts and techniques used in the transmission of data over telephone and cable networks. To facilitate the transmission of data over these networks, various protocols and standards have been developed. These include the asynchronous transfer mode (ATM) protocol, the transmission control protocol/Internet protocol (TCP/IP), and the digital subscriber line (DSL) standard. These protocols and standards help to ensure that data is transmitted efficiently and reliably over the network.

KEYWORDS:

Cable Network, Control Protocol, Data Transmission, DSL, Internet Protocol.

INTRODUCTION

The development of data communication has come a long way, from the first electronic mail sent in the early 1970s to the current era of ubiquitous, high-speed internet connectivity. However, in the early days of data communication, there were few dedicated data networks, and data was typically transmitted over telephone and cable networks, which were designed primarily for voice and television transmission, respectively [1], [2] . This paper will explore the use of telephone and cable networks for data transmission, including the underlying technologies, advantages, and limitations of each approach.

The telephone network was the first widely deployed network infrastructure and was designed primarily for voice communication. However, in the early days of data communication, modems were used to convert digital data into analog signals that could be transmitted over the telephone network. Modems use a technique called modulation to convert the digital data into a form that can be transmitted over an analog medium, such as a telephone line. Modems transmit data using a series of sound waves that are modulated to represent digital data. These waves are sent over the telephone line and are received by a modem on the other end, which demodulates the waves to recover the original digital data. Modems are typically rated by their data transfer rate, which determines the maximum speed at which data can be transmitted over the telephone network.

One advantage of using the telephone network for data transmission is its wide availability. Telephone lines are available in most populated areas, making it possible to connect to the internet from almost anywhere. Additionally, the cost of using the telephone network for data transmission is relatively low, as most users are already paying for a telephone line and can use it for data transmission at no additional cost[3]. However, there are also some limitations associated with using the telephone network for data transmission. One major limitation is the relatively low data transfer rates that can be achieved. Modems are limited by the maximum frequency that can be transmitted over the telephone line, which limits the maximum data transfer rate. Additionally, because the telephone network was not designed for data transmission, it can be prone to errors and noise that can degrade the quality of the data transmission.

Cable networks were originally designed to transmit television signals and were later adapted for broadband internet access. Cable networks use a different technology than telephone networks for data transmission, called broadband internet access. This technology uses a coaxial cable to transmit data, rather than a telephone line. Broadband internet access uses a technique called frequency-division multiplexing (FDM) to transmit data over the cable network. FDM divides the available frequency range of the cable into multiple channels, each of which can be used to transmit data. Each channel is modulated with a different frequency, and the resulting modulated signals are combined and transmitted over the cable.

One advantage of using a cable network for data transmission is the higher data transfer rates that can be achieved. Cable networks are capable of much higher data transfer rates than telephone networks, which allows for faster internet access and the ability to transmit large files, such as video and audio files, more quickly. Additionally, cable networks are less prone to errors and noise than telephone networks, which can result in higher quality data transmission [4], [5]. However, there are also some limitations associated with using cable networks for data transmission. One major limitation is the limited availability of cable networks, as they are typically only available in populated areas. Additionally, the cost of using cable networks for data transmission can be relatively high, as users may need to pay for both a cable television subscription and a broadband internet access subscription can be transmitted over the network. Cable networks generally offer much higher data transfer rates than telephone networks, which can be a significant advantage for applications that require high-speed data transmission, such as streaming media and online gaming.

Another important factor to consider is availability. Telephone networks are widely available, as most populated areas have access to a telephone line. Cable networks, on the other hand, are typically only available in urban and suburban areas, which can limit their usefulness for rural or remote areas. Reliability is also an important consideration. Telephone networks can be prone to errors and noise that can degrade the quality of the data transmission, while cable networks are generally more reliable and less prone to errors and noise. The cost of using the network for data transmission is also an important consideration. Telephone networks are typically less expensive to use, as users are already paying for a telephone line and can use it for data transmission at no additional cost. Cable networks, on the other hand, require users to pay for both a cable television subscription and a broadband internet access subscription, which can be more expensive. Security is another factor to consider. Both telephone and cable networks are vulnerable to network attacks, such as hacking and denial-of-service attacks. However, cable

networks are generally considered to be more secure than telephone networks, as they use encryption and other security measures to protect against network attacks.

DISCUSSION

Voice communication was the initial purpose for which telephone networks were developed. The dial-up modem was developed as a consequence of the necessity to transmit digital data. High-speed downloading and uploading became necessary with the development of the Internet. The modem was just too sluggish. The digital subscriber line is a new technology that the telephone companies have implemented (DSL). Despite the fact that dial-up modems are still widely used around the globe, DSL offers substantially quicker access to the Internet over the telephone network. We first go over the fundamental organisation of the telephone network in this chapter. The usage of these networks for Internet access using dial-up and DSL technologies is then shown. Initially, the purpose of cable networks was to provide users who could not receive TV signals due to geographical obstacles like mountains access to TV shows [6].

Subsequently, others who only want a stronger signal started to use the cable network. Moreover, cable networks made it possible to connect wirelessly to distant broadcasting stations. By using some of the channels that were initially intended for television, cable TV has found a lucrative market in the provision of Internet access. After a discussion of the fundamental design of cable networks, we go into how cable modems may provide a fast connection to the Internet. Circuit switching is used in telephone networks. The late 1800s saw the commencement of the telephone network. The whole network, known as the plain old telephone system (POTS), was initially an analogue system that transmitted voice through analogue signals. In the 1980s, when the computer age came into being, the network started to transmit data in addition to speech. The telephone network has experienced several technological upgrades during the last ten years. The network currently has both digital and analogue components.

Local loops, trunks, and switching offices make up the three main parts of the telephone network. There are many levels of switching offices in the telephone network, including end offices, tandem offices, and regional offices. The local loop, a twisted-pair cable that links the subscriber phone to the closest end office or local central office, is one part of the telephone network. The local loop, when used for speech, has a bandwidth of 4000 Hz (4 kHz) (4 kHz). It is fascinating to examine the telephone number connected with each local loop. A local phone number's first three digits identify the office, while the next four digits identify the local loop number. Trunks are the transmission medium used for interoffice communication. By multiplexing, a trunk often manages hundreds or thousands of connections. Often, satellite connections or optical fibres are used for transmission.The telephone company uses switches at a switching office to prevent establishing a permanent physical connection between any two customers. Several local loops or trunks are connected via a switch, enabling connections between various subscribers.

Intra-LATA services refer to the services provided by common carriers (telephone companies) inside a LATA. A local exchange carrier is the company in charge of these services (LEC). Prior to the Telecommunications Act of 1996 only one carrier was allowed to provide intra-LATA services. As a monopoly, this was. From 1996, a LATA might have more than one carrier offering services there. The incumbent local exchange carrier is the company that supplied services before to 1996 and is the owner of the cabling infrastructure (local loops) (ILEC). Competitive local exchange carriers are the new carriers that may provide services (CLECs).

Communication inside a LATA is handled by end switches and tandem switches to save the expense of additional cable. Toll-free calls are those that can be made using just end offices. A fee is applied to calls that must pass through a tandem office (intra-LATA toll office) [7].

Interexchange carriers conduct the services between LATAs (IXCs). These carriers, often known as long-distance providers, provide communication services between two clients in various LATAs. Under the statute of 1996 (see Appendix E), any carrier, even those engaged in intra-LATA services, is permitted to provide these services. The playing field is open. AT&T, MCI, WorldCom, Sprint, and Verizon are among of the carriers that provide inter-LATA services. Long-distance carriers known as IXCs provide a range of data communications services, including phone service. Most phone calls that pass via an IXC are digital, and the carriers use a variety of networks to provide their services.

As we previously mentioned, numerous LECs (including one ILEC and maybe more than one CLEC) can provide intra-LATA services. We also said that a number of IXCs may provide inter-LATA services. What kind of interactions occur between these carriers? The response is via a point of presence, a switching office (POP). Any IXC that wishes to provide interLATA services in a LATA is required to have a POP there. To ensure that every subscriber has access to every POP, the LECs that provide services within the LATA must offer connections. An end switch is used as the initial point of connection for a subscriber who has to connect to another subscriber, and the POP is reached either directly or through a tandem switch after that. The call now travels from the subscriber's selected IXC's POP in the source LATA to that IXC's POP in the destination LATA. The IXC's network is used to carry the call once it has gone through its toll office.

The first telephone network employed a circuit-switched network with dedicated lines to transfer voice communication since multiplexing had not yet been developed. A circuit-switched network requires the setup and takedown phases to create and close pathways between the two communication parties. This job was first carried out by human operators. Each subscriber was linked to the operator room, which served as a hub. A subscriber dialed the operator after picking up the receiver (off-hook) and asking to speak to another subscriber. After hearing the caller and learning who was being contacted, the operator linked the two using a wire with two plugs placed into the appropriate two jacks [8]. This resulted in the creation of a specialized circuit. Once the discussion was over, one of the participants told the operator to cut the circuit. Since the same circuit may be used for both signaling and speech transmission, this sort of signaling is known as in-band signaling.

The signaling system eventually become automated. There are now rotary telephones that transmit a digital signal that specifies each digit of a multi digit telephone number. The telephone companies' switches employed digital signals to establish a link between the caller and the people being contacted. There was a combination of in-band and out-of-band signals. The 4-kHz speech channel was further utilized for in-band signaling. A part of the voice channel's bandwidth was utilized for signaling during out-of-band signaling; the voice bandwidth and the signaling bandwidth were distinct. The signaling system's capabilities expanded as telephone networks developed into sophisticated networks. In addition, the signaling system provide the dial tone, ring tone, and busy tone.

It was necessary to provide a distinct network for signaling as a consequence of these challenging duties. A signaling network and a data transfer network are two examples of modern

telephone networks, respectively. In contemporary telephone networks, data transport and signaling are carried out by distinct networks; signaling is handled by a third network. Yet, we must make a specific point here. The two networks may utilize different channels of the same connection in certain portions of the system, despite the fact that they have distinct physical links elsewhere.

While it may also be a packet-switched network, the data transfer network that can transmit multimedia data today is, for the most part, a circuit-switched network. The model and protocols used by this network are the same as those used by other networks covered in this book. A packet-switched network with layers like to those in the OSI model or Internet model, which were addressed, makes up the signaling network, which is the focus of this part. The nature of signaling makes it more suitable for a multi-layer packet-switching network. For instance, it is simple to encapsulate the information required to transmit a phone number in a packet that also contains all the error-control and addressing data.

The signal points are linked to the user's phone or PC (SPs). For both networks, there is a common connection between the telephone set and SP. Signal transport ports (STPs), which are nodes in the signaling network, are used to receive and transmit signaling messages. A service control point (SCP) is another component of the signaling network that manages the network's overall functionality. To offer saved data on the complete signaling network, other systems.

MTP Level 2 for Data Link Layer Typical data link layer functions like packetizing, utilizing source and destination addresses in the packet header, and CRC for error checking are all provided by the MTP level 2 layer. MTP Level 3 for Network Layer the MTP level 3 layer uses a datagram-based switching strategy to offer end-to-end connection. Signal packets are routed by switches and routers from the source to the destination. Setting up voice calls is done using the telephone user port (TUP). The calls are routed once it gets the phoned numbers. A computer's application software may call a process on another computer by using the Transaction Capabilities Application Port (TCAP), which offers remote calls. TUP may be replaced with an ISDN user port (ISUP) to provide services like those of an ISDN network. These services are still offered right now. These services fall into one of two categories: analogue switched services or analogue leased services. Switched Analog Services When using a home phone, this is the dial-up service that is most often utilized. An analogue signal on a local loop typically has a bandwidth of 0 to 4000 Hz.

The cost of a local call service is typically a fixed monthly fee, however in certain LATAs, the carrier may charge for a single call or a group of calls. The justification for a non-flat-rate fee is to provide less expensive service to clients who do not place a lot of calls. Both intra-LATA and inter-LATA calls are toll calls. A call may go via a tandem office (toll office) if the LATA is big geographically, and the subscriber will be charged for the call. Inter-LATA calls are considered long distance calls and are priced accordingly. The 800 service is another option. The 800 service may be requested by a subscriber often an organization if it wants to provide free connections to other subscribers typically consumers. The call in this instance is free for the caller is responsible for payment. This service is used by a business to get people to call. The cost is less than what you would pay for an ordinary long-distance call.

The antithesis of the 800 service is the wide-area telephone service (WATS). The latter are incoming calls that the company has paid for, whilst the former are outgoing calls. Regular toll calls may be replaced with this service for less money; fees are calculated depending on the

volume of calls. Outbound calls to one state, many states, or the whole nation may be chosen for the service, and prices will be paid appropriately. As incoming calls to a subscriber, 900 services are similar to 800 services. The call is paid for by the caller, unlike the 800 service, and is often far more costly than a typical long-distance call. The carrier levies two costs: the first is the long-distance toll, and the second is the cost of each call to the caller.

Leased Service in Analog Customers who choose for an analogue leased service have the option to rent a line that is permanently linked to another customer and is commonly referred to as a dedicated line. Customers see the connection as a single line even if the connection still goes through switches in the telephone network since the switch is constantly closed and no dialing is required. Lately, telephone companies started providing users with digital services. Compared to analogue services, digital services are less susceptible to noise and other types of interference. Service Switched/56 an analogue switched line has a digital equivalent called switched/56 service. It is a switched digital service that supports up to 56 kbps of data rate. Both parties must sign up for this service in order to converse. Even if the caller is using a modem, a caller with standard telephone service cannot connect to a phone or computer using switched/56 service. Overall, the telephone companies' digital and analogue services constitute two quite distinct business sectors. Subscribers do not need modems to send digital data since a switched! 56 service already has a digital line.

They do, however, need an additional gadget known as a digital service unit (DSU). Electronic Data Service The analogue leased line's digital equivalent, known as digital data service (DDS), has a maximum transfer rate of 64 kbps. Conventional telephone lines have a bandwidth of 3000 Hz and can transmit frequencies between 300 and 3300 Hz. All of this spectrum is utilized for speech transmission, which can tolerate significant amounts of interference and distortion without losing clarity. Yet, as we've seen, data signals need a greater level of precision to guarantee integrity. Thus, the boundaries of this range are not utilized for data transfers for reasons of safety. Generally speaking, we may state that the cable bandwidth must be less than the signal bandwidth. A telephone line's effective bandwidth, which covers the frequency range of 600 to 3000 Hz, is 2400 Hz. Take note that certain modern telephone connections can handle more bandwidth than older ones. It is also important to note that as technology continues to evolve, the distinctions between telephone and cable networks are becoming increasingly blurred. Many telephone networks are now offering broadband internet access and other data transmission services, while cable networks are expanding their coverage areas to include more rural and remote areas.

In addition, the emergence of wireless networks, such as cellular networks and Wi-Fi networks, is providing new options for data transmission that are not limited by the physical infrastructure of telephone and cable networks [9][10]. These networks offer the potential for greater mobility and flexibility, as users can access the network from virtually anywhere. Despite these advances, however, telephone and cable networks will likely continue to play an important role in data transmission for years to come. Their widespread availability, established infrastructure, and relatively low cost make them a reliable and accessible option for many applications. As data communication continues to evolve, it will be important for developers and network operators to stay up-to-date with the latest technologies and best practices in order to ensure the most effective and efficient use of network infrastructure. By continuing to push the boundaries of what is possible with data communication, we can unlock new opportunities for innovation and growth in virtually every area of society.

CONCLUSION

The use of telephone and cable networks for data transmission has played a significant role in the development of data communication. These networks offer several advantages such as widespread availability, established infrastructure, and relatively low cost. Telephone networks were the first widely deployed network infrastructure and were used for data transmission through the use of modems. Cable networks were originally designed for television transmission and were later adapted for broadband internet access. When comparing the use of telephone and cable networks for data transmission, there are several key factors to consider, including data transfer rate, availability, reliability, cost, and security. While cable networks generally offer higher data transfer rates and are more reliable than telephone networks, they can be more expensive to use and are typically only available in urban and suburban areas. Telephone networks, on the other hand, are widely available and less expensive to use, but are generally less reliable and offer lower data transfer rates.

REFERENCES

[1] T. Network, "CHAPTER 9 Using Telephone and Cable Networks for Data Transmission," *Library (Lond).*, 2006.

[2] M. Islam and S. Jin, "An Overview Research on Wireless Communication Network," *Adv. Wirel. Commun. Networks*, 2019, doi: 10.11648/j.awcn.20190501.13.

[3] G. Mantokoudis, R. Koller, J. Guignard, M. Caversaccio, M. Kompis, and P. Senn, "Influence of telecommunication modality, internet transmission quality, and accessories on speech perception in cochlear implant users," *J. Med. Internet Res.*, 2017, doi: 10.2196/jmir.6954.

[4] J. Shin, K. Cho, D. Lee, and T. Kim, "A Conversion Protocol for 2W Telephone Signal over Ethernet in a Private PSTN," *J. Korea Inst. Mil. Sci. Technol.*, 2021, doi: 10.9766/kimst.2021.24.6.645.

[5] R. A. Siswanto, C. Anam, and S. -, "RANCANG BANGUN INTERNET SERVICE PROVIDER (ISP) LOKAL DENGAN JARINGAN WIRRELESS DAN MIKROTIK OS," *SAINTEKBU*, 2018, doi: 10.32764/saintekbu.v10i2.211.

[6] V. Balashov, A. Lashko, L. Liakhovetsky, V. Oreshkov, and V. Skurikhin, "Evaluation of the Efficiency of the VDSL2 Technology Implementation on the PJSC «Ukrtelecom» Network," *Metrol. instruments*, 2018, doi: 10.33955/2307-2180(5)2018.15-22.

[7] V. D and K. R, "FUZZY SHORTEST ROUTE ALGORITHM FOR TELEPHONE LINE CONNECTION USING THE LC-MST ALGORITHM," *Kongunadu Res. J.*, 2015, doi: 10.26524/krj93.

[8] V. D and K. R, "A STUDY ON FUZZY SHORTEST ROUTE ALGORITHM FOR TELEPHONE LINE CONNECTION," *Kongunadu Res. J.*, 2015, doi: 10.26524/krj66.

[9] M. N. O. Sadiku and C. Aduba, "Cable modem technology," *IEEE Potentials*, 2000, doi: 10.1109/45.877862.

[10] R. Bhoyar, M. Ghonge, S. G.-I. J. of Advanced, and U. 2013, "Comparative Study on IEEE Standard of Wireless LAN/Wi-Fi 802.11 a/b/g/n," *Int. J. Adv. Res. Electron. Commun. Eng.*, 2013.

CHAPTER 16

DATA LINK LAYER ERROR DETECTION: A COMPARATIVE STUDY ON HAMMING, AND PARITY CHECK TECHNIQUES FOR ROBUST AND RELIABLE DATA COMMUNICATION

Alka Verma, Associate Professor
Department of Electronics and Communication Engineering, Teerthanker Mahaveer University, Moradabad, Uttar Pradesh, India
Email Id- alkasinghmail@rediffmail.com

ABSTRACT:

The Data Link Layer is the second layer of the OSI (Open Systems Interconnection) model, which is responsible for reliable and efficient data transfer between adjacent network nodes. It provides services to the Network Layer, which uses it to transmit packets of data over the physical network. The Data Link Layer is responsible for error detection, flow control, and framing. It ensures that the data packets are transmitted reliably and without errors. The layer also provides a mechanism to detect errors that may occur during the transmission of data, such as bit errors or lost packets.

KEYWORDS:

Data Link, Lost Packets, OSI, Network Layer, Transmit Packets.

INTRODUCTION

The Data Link Layer is the second layer of the OSI model, which is responsible for transmitting data between two adjacent nodes over a physical medium. One of the primary functions of the Data Link Layer is to ensure reliable transmission of data between the sender and the receiver. To achieve this, error detection and correction techniques are employed in the Data Link Layer. Error detection refers to the process of identifying errors that may occur during the transmission of data. There are two main types of errors that may occur during data transmission: single-bit errors and burst errors. A single-bit error occurs when a bit in the transmitted data is flipped, while a burst error occurs when a group of consecutive bits is corrupted [1], [2]. There are several error detection techniques that can be used in the Data Link Layer to detect these errors. Some of the most commonly used techniques are:

1. **Parity checking:** Parity checking is a simple error detection technique that adds an extra bit to each byte of data transmitted. The extra bit, known as the parity bit, is set to 1 or 0 so that the total number of 1s in each byte including the parity bit is even or odd. The receiver then checks the parity bit to determine if there has been an error in transmission. If the number of 1s in the received byte is not the same as the expected parity, then an error is detected.
2. **Checksum:** A checksum is a value calculated from a block of data using a mathematical algorithm. The sender adds the checksum value to the end of the data block before transmission. The receiver then recalculates the checksum value using the same algorithm

and compares it to the received checksum value. If the two values match, then the data has been transmitted without errors. If the values do not match, then an error is detected.

3. **Cyclic Redundancy Check (CRC):** CRC is a more sophisticated error detection technique that uses polynomial division to calculate a remainder value that is added to the end of the data block before transmission. The receiver performs the same polynomial division using the same polynomial and checks if the remainder value is zero. If the remainder is zero, then the data has been transmitted without errors. If the remainder is non-zero, then an error is detected.
4. **Hamming Code:** Hamming Code is an error detection and correction technique that uses extra bits to detect and correct single-bit errors. The sender adds the extra bits to the data block before transmission, and the receiver checks the extra bits to detect and correct errors.

These techniques are designed to detect errors, but they do not correct them. Error correction can be achieved using techniques like retransmission, forward error correction, or automatic repeat request (ARQ). Retransmission involves resending the data block that was detected as being corrupted or lost during transmission. This approach can be time-consuming, especially for long data blocks, but it is effective for correcting errors [3].

Forward Error Correction (FEC) is a technique that involves adding extra information to the data block before transmission so that errors can be corrected at the receiver without the need for retransmission. The receiver uses the extra information to correct any errors in the received data. Automatic Repeat Request (ARQ) is a technique that combines error detection and retransmission. The receiver sends an acknowledgement to the sender for each data block received successfully. If an error is detected, the receiver sends a negative acknowledgement (NACK) to the sender, requesting that the data block be resent. The sender then resends the data block until it receives a positive acknowledgement (ACK) from the receiver.

Cyclic Redundancy Check (CRC), and Hamming Code. These techniques are designed to detect errors, but they do not correct them. Error correction techniques like retransmission, Forward Error Correction (FEC), and Automatic Repeat Request (ARQ) can be used to correct errors and ensure reliable transmission of data. Retransmission is the simplest error correction technique and involves resending the data block that was detected as being corrupted or lost during transmission. The receiver acknowledges the successful receipt of each data block, and if an error is detected, the sender retransmits the data block until it is received successfully.

Forward Error Correction (FEC) is a more complex error correction technique that involves adding extra information to the data block before transmission so that errors can be corrected at the receiver without the need for retransmission. The extra information, also known as redundant bits, can be used to detect and correct errors in the received data. One example of a FEC technique is Reed-Solomon coding, which is commonly used in satellite communication and other high-noise environments.

Automatic Repeat Request (ARQ) is a technique that combines error detection and retransmission. The receiver sends an acknowledgement to the sender for each data block received successfully. If an error is detected, the receiver sends a negative acknowledgement

(NACK) to the sender, requesting that the data block be resent. The sender then retransmits the data block until it receives a positive acknowledgement (ACK) from the receiver [4], [5].

DISCUSSION

There are several variants of ARQ, including Stop-and-Wait ARQ, Go-Back-N ARQ, and Selective Repeat ARQ. Stop-and-Wait ARQ is the simplest variant and involves transmitting a single data block at a time and waiting for an acknowledgement before transmitting the next data block. Go-Back-N ARQ and Selective Repeat ARQ are more complex variants that allow for the transmission of multiple data blocks before waiting for an acknowledgement.

In addition to these error detection and correction techniques, the Data Link Layer also uses flow control mechanisms to ensure that data is transmitted at a rate that the receiver can handle. Two commonly used flow control techniques are Stop-and-Wait Flow Control and Sliding Window Flow Control. Stop-and-Wait Flow Control is a simple technique that involves transmitting a single data block at a time and waiting for an acknowledgement before transmitting the next data block. This technique ensures that the receiver can handle the data at the same rate as the sender.

Sliding Window Flow Control is a more complex technique that allows for the transmission of multiple data blocks before waiting for an acknowledgement. The sender maintains a buffer of unacknowledged data blocks, and the receiver sends an acknowledgement for each data block received successfully. The size of the buffer, also known as the window size, can be adjusted dynamically based on the network conditions [6], [7].

Networks must be capable of accurately transferring data from one device to another. A system must ensure that the data received and those transferred are same for the majority of applications. Data can become corrupted while being transmitted from one node to the next. A message's components might change according to a variety of events. Some Some apps are tolerant of very little errors. For instance, occasional mistakes in audio or video transmissions could be acceptable, but we need a very high degree of accuracy when transmitting text. Let's start by talking about a few difficulties that are either directly or indirectly connected to mistake correction and detection.

Every time bits go from one location to another, interference might produce unexpected changes. The signal's form may alter as a result of this interference. A 0 may turn into a 1 or an O into a 1 in a single-bit mistake. A burst mistake involves the alteration of many bits. For a transmission with a data rate of 1200 bps, for instance, a 11100 s burst of impulse noise might alter all or part of the 12 bits of information. When a single bit of a given data unit such a byte, character, or packet) is altered from 1 to 0 or from 0 to 1, it is referred to as a single-bit error. Burst errors happen more often than single-bit errors. Since that noise often lasts for longer than one bit, when it impacts data, it typically affects many bits. The amount of bits that are impacted depends on the noise duration and data rate. For instance, a noise of 11100 s may impact 10 bits while delivering data at 1 kbps, whereas the same noise can affect 10,000 bits when sending data at 1 Mbps.

Redundancy is the key idea in mistake detection or correction. We need to provide a few additional bits along with our data in order to be able to recognize or fix problems. The transmitter adds and the recipient subtracts these extraneous bits. They enable the receiver to identify or fix damaged bits. Error rectification is more challenging than error detection. When

detecting errors, our primary concern is determining if any errors have taken place. Simple yes or no answers are provided. Even the quantity of mistakes doesn't matter to us. For us, a burst error is the same as a single-bit error.We need to know the precise amount of corrupted bits and, more crucially, where in the message they are located in order to do error repair. Important considerations are the quantity of mistakes and the size of the message. Eight different error sites must be taken into account while fixing a single mistake in an 8-bit data unit, and 28 different places must be thought about when fixing two faults in the same size of data unit. You may imagine how challenging it would be for the receiver to detect 10 faults in a data unit with 1000 bits.

Error repair may be done using two major techniques. The procedure of forward error correction involves the receiver attempting to decipher the message using redundant bits. As we will see later, if there are few mistakes, this is feasible. Retransmission correction is a method where the sender is requested to transmit the message again after the recipient discovers a mistake. Repeated resending occurs until the recipient receives a message that they feel is error-free usually, not all errors can be detected.

Several coding systems are used to achieve redundancy. Via a procedure that establishes a connection between the redundant bits and the real data bits, the sender inserts superfluous bits. To find or fix faults, the receiver examines the connections between the two sets of bits. In every coding system, the proportion of superfluous bits to data bits and the process's stability are crucial considerations. Block coding and convolution coding are the two basic categories into which coding techniques may be divided. Convolutional coding is more complicated and falls beyond the purview of this book, therefore we will focus on block coding in this one. Let's quickly go over modular arithmetic before we wrap up this subject. This idea is fundamental to computer science in general and error detection and correction in particular. Our goal in this section is to offer a backdrop for the things addressed in this chapter, not to go extensively into the mathematics surrounding this subject [8].

Just a few integers are used in modular arithmetic. A modulus N is the utmost limit that we specify. Then, we limit our usage to the integer range of 0 to N - I, inclusive. This is arithmetic in modulo-N. We only utilize the numbers 0 to 11, for instance, if the modulus is 12. Our clock mechanism is an illustration of modulo arithmetic. It is based on modulo-12 arithmetic, in which 12 is used in place of O. If a number is larger than N in a modulo-N system, it is divided by N, and the remainder provides the answer. If it is negative, the necessary number of Ns are added in order to make it positive. Think about our clock system once again.

If a project starts at 11 a.m. and takes 5 hours to complete, we may state that it will be done by 4 p.m. if we are in the military since 4 is the remaining 16/12 hours. With block coding, we separate our message into data words, which are blocks of k bits apiece. Each block is given an additional r superfluous bits to make the length n = k + r. Code words are the n-bit blocks that are the outcome. We shall talk about how the additional r bits are selected or computed later. The fact that we have a collection of data words, each of size k, and a set of code words, each of size n, is crucial for the time being. By using k bits, we can combine 2k data words, and when using n bits, we can combine 2n code words.

The number of potential code words exceeds the number of potential data words because n > k. The same data word is always encoded as the same code word in a one-to-one block coding procedure. This indicates that we have 2n–2k unutilized code words. We refer to them as invalid

or unlawful code words. Error rectification is far more challenging than error detection, as we have already shown. In order to repair a mistake, the receiver must locate (or guess) the original code word that was transmitted; with error detection, the receiver just has to be aware that the code word they have just received is wrong. We may claim that error repair requires more redundant bits than error detection.

While the checker functions are far more complicated, we can see that the concept is the same as error detection. Error rectification is more difficult than mistake detection since a choice must be made. The receiver must determine which valid code word was really transmitted when a received code word is invalid. The choice is supported by the idea of territory, a restricted region around the code word each legal code word has a defined range of use. In order to define each region, we use a geometrical technique. Assume, for example, that a code word x is corrupted by t bits or fewer. We assume that each legitimate code word has a circular territory with a radius of t and that the valid code word is at the. Then, within or outside of this circle, this distorted code word may be found. When a code word from this region is received, the receiver determines that the original code word is the one in the middle. The choice is incorrect if more than t mistakes have not happened, as we have assumed.

Its geometric interpretation is seen the distance between all legal block codes is often represented graphically as a sphere. Today's block codes almost all fall under the category of linear block codes. Because of their structure, nonlinear block codes are more difficult to theoretically analyse and put into practice, which limits their application for error detection and correction. Thus, our focus is on linear block codes. It is beyond the purview of this book to discuss the formal formulation of linear block codes since it needs an understanding of abstract algebra, specifically Galois fields. Hence, we provide a loose definition. For our purposes, a linear block code is one in which the exclusive OR of two valid code words results in the creation of another valid code word (addition modulo-2). The smallest Hamming distance for a linear block coding may be easily determined. The amount of is in the nonzero valid codeword with the fewest is called the lowest Hamming distance.

The nonzero codewords in our first code have is numbers of 2, 2, and 2. Hence, dmin = 2 is the minimal Hamming distance. The nonzero codewords in our second code have is numbers 3, 3, and 4. Dmin = 3 is the result of this code. Now, let's demonstrate some linear block codes. These codes are simple because it is simple to locate the encoding and decoding algorithms and assess how well they work.The straightforward parity-check code is maybe the most well-known error-detecting code. A k-bit data word is converted into an n-bit code word in this code, where n = k + 1. To make the total number of is in the code word even, the additional bit, referred to as the parity bit, is chosen. We talk about the even situation even though some implementations call for an odd number of Is. As the category's minimal Hamming distance is 2, the code is a single-bit error-detecting code and cannot repair any errors. A straightforward parity-check code is an error-detection code using a single bit, where n = k + 1, and dmin = 2.

The generator used by the encoder creates a parity bit roo using a copy of a 4-bit dataword (ao, aI', a2', and a3). The 5-bit codeword is made up of the dataword bits and the parity bit. The codeword's Is are evenly spaced thanks to the parity bit [9]. The two-dimensional parity check is a superior method. This approach arranges the dataword in a table (rows and columns). One parity-check bit is computed for each row and each column. The receiver then receives the whole table and determines the syndrome for each row and column. The two-dimensional parity check

may find up to three faults anywhere in the table, arrows indicate the positions of the newly formed nonzero syndromes. However it's possible that 4 bit mistakes go undetected.

Let's now talk about the Hamming code subclass of error-correcting codes. As the original design of these programmed had dim = 3, they could either identify up to two problems or fix only one.

The single-bit error-correcting code is the subject of our discussion, even though certain Hamming codes may correct multiple errors. Let's start by determining how n and k are related in a Hamming code. Selecting an integer m >= 3 is necessary. Next, using mas n = 2m - 1 and k:: n - m, the values of n and k are determined. The check bit count is r = m. Since there is either no error or a parity bit mistake, the four scenarios indicated in Table 10.5 are unimportant to the generator. To discover the right data word in the other four situations, one of the bits must be flipped (turned from 0 to 1 or 1 to 0). Based on the calculations for the syndrome bit, Table 10.5's syndrome values. For instance, if qo is incorrect, so is the only bit that is impacted; as a result, the symptom is 001. So and s1 are the bits that are impacted if b2 is incorrect; as a result, OIl is the syndrome. Similar to how all three syndrome bits are impacted if bI is incorrect, the syndrome is 111. Now, we need to place particular emphasis on two aspects. First, the generated data word could not be the correct one if there are two transmission mistakes. Second, a new architecture is required if we want to utilise the aforementioned code for error detection.

CONCLUSION

The Data Link Layer is an important layer in the OSI model, responsible for ensuring reliable transmission of data over a communication network. One of its key functions is error detection, which is achieved through the use of various techniques such as parity checking, checksum, CRC, and Hamming Code [10], [11] . These techniques detect errors in the data transmitted and alert the receiver or sender to take necessary actions such as retransmission, error correction or request for resending the data. To further enhance reliability, error correction techniques such as retransmission, Forward Error Correction (FEC), and Automatic Repeat Request (ARQ) are employed, and flow control mechanisms are used to regulate the rate of data transmission to avoid data loss due to receiver buffer overflow.

REFERENCES

[1] A. Azahari, R. Alsaqour, M. Uddin, and M. Al-Hubaishi, “Review of error detection of data link layer in computer network,” *ARPN J. Eng. Appl. Sci.*, 2014.

[2] A. Tandon, T. J. Lim, and U. Tefek, “Sentinel based malicious relay detection in wireless IoT networks,” *J. Commun. Networks*, 2019, doi: 10.1109/JCN.2019.000049.

[3] U. Amirsaidov and A. Qodirov, “A Packet Delay Assessment Model in the Data Link Layer of the LTE,” *Int. J. Informatics Vis.*, 2021, doi: 10.30630/JOIV.5.4.601.

[4] M. Usman, V. Muthukkumarasamy, and X. W. Wu, “Mobile agent-based cross-layer anomaly detection in smart home sensor networks using fuzzy logic,” *IEEE Trans. Consum. Electron.*, 2015, doi: 10.1109/TCE.2015.7150594.

[5] S. Bourebia *et al.*, “A belief function-based forecasting link breakage indicator for VANETs,” *Wirel. Networks*, 2020, doi: 10.1007/s11276-019-01973-0.

[6] S. H. Islam *et al.*, "On Secrecy Performance of Mixed Generalized Gamma and Málaga RF-FSO Variable Gain Relaying Channel," *IEEE Access*, 2020, doi: 10.1109/ ACCESS.2020.2998742.

[7] C. Mendoza and M. P. McGarry, "The Network Link Outlier Factor (NLOF) for Fault Localization," *IEEE Open J. Commun. Soc.*, 2020, doi: 10.1109/OJCOMS.2020.3025663.

[8] N. Jafarzadeh, M. Palesi, S. Eskandari, S. Hessabi, and A. Afzali-Kusha, "Low Energy yet Reliable Data Communication Scheme for Network-on-Chip," *IEEE Trans. Comput. Des. Integr. Circuits Syst.*, 2015, doi: 10.1109/TCAD.2015.2440311.

[9] D. M. Pham and S. M. Aziz, "Object extraction scheme and protocol for energy efficient image communication over wireless sensor networks," *Comput. Networks*, 2013, doi: 10.1016/j.comnet.2013.07.001.

[10] M. A. Management, "4 . Media Access Control," *ReVision*, 2005.

[11] W. Aman *et al.*, "Securing the insecure: A first-line-of-defense for body-centric nanoscale communication systems operating in thz band," *Sensors*, 2021, doi: 10.3390/s21103534.

CHAPTER 17

ANALYSIS AND COMPARISON OF DATA LINK CONTROL PROTOCOLS FOR RELIABLE DATA TRANSFER IN COMMUNICATION NETWORKS

Neeraj Kaushik, Assistant Professor
Department of Electronics and Communication Engineering,
Teerthanker Mahaveer University, Moradabad, Uttar Pradesh, India
Email Id- neeraj1604@gmail.com

ABSTRACT:

Data Link Control (DLC) is a critical function of the Data Link Layer in computer networking, responsible for the reliable transmission of data over a communication network. The DLC layer is responsible for establishing, maintaining, and terminating a logical link between two nodes, as well as for detecting and correcting errors in data transmission. DLC protocols employ several error detection and correction techniques, including parity checking, checksum, and cyclic redundancy check (CRC), and Hamming Code, to ensure the accuracy and integrity of the data transmitted. Error correction techniques such as retransmission, Forward Error Correction (FEC), and Automatic Repeat Request (ARQ) are also used to correct errors and ensure reliable data transmission.

KEYWORDS:

Automatic Repeat Request, Cyclic redundancy check, Data Link Control, Forward Error Correction, Logical Linking.

INTRODUCTION

Data Link Control (DLC) is a sub-layer of the Data Link Layer in the OSI model. The Data Link Layer is the second layer in the OSI model and is responsible for providing reliable data transfer over a physical link. The Data Link Layer is responsible for error detection and correction, flow control, and framing[1]–[3] . The Data Link Control (DLC) sub-layer is responsible for providing reliable data transfer between two adjacent nodes.

The Data Link Control (DLC) sub-layer provides the following services:

1. **Framing:** The DLC sub-layer is responsible for framing the data into packets that can be transmitted over the physical link. The frames include a header and a trailer that contains control information such as sequence numbers, acknowledgments, and error detection codes.
2. **Error detection and correction:** The DLC sub-layer is responsible for detecting and correcting errors that may occur during data transmission. The most common error detection and correction method used by the DLC sub-layer is the Cyclic Redundancy Check (CRC).

3. **Flow control:** The DLC sub-layer is responsible for controlling the flow of data between two adjacent nodes. Flow control ensures that the receiver is able to receive the data at a rate that it can handle. The most common flow control mechanism used by the DLC sub-layer is the sliding window protocol.
4. **Access control:** The DLC sub-layer is responsible for controlling access to the physical link. The most common access control mechanism used by the DLC sub-layer is the Carrier Sense Multiple Access with Collision Detection (CSMA/CD) protocol.

The DLC sub-layer provides these services by implementing various protocols. The most common DLC protocols are:

1. **High-Level Data Link Control (HDLC):** HDLC is a bit-oriented protocol that was developed by the International Organization for Standardization (ISO). HDLC is widely used in networking applications and is the basis for many other protocols, including the Point-to-Point Protocol (PPP) and Frame Relay.
2. **Point-to-Point Protocol (PPP):** PPP is a protocol used to establish a direct connection between two nodes. PPP is commonly used for dial-up connections and is used by Internet Service Providers (ISPs) to provide Internet access.
3. **Serial Line Internet Protocol (SLIP):** SLIP is a protocol used to establish a direct connection between two nodes over a serial line. SLIP is commonly used for connecting two computers directly or for connecting a computer to a router.
4. **Ethernet:** Ethernet is a protocol used for local area networks (LANs). Ethernet uses CSMA/CD for access control and is used by most LANs.
5. **Token Ring:** Token Ring is a protocol used for LANs. Token Ring uses a token-passing mechanism for access control.

The DLC sub-layer also provides error control through a variety of techniques. These techniques include:

1. **Parity checking:** Parity checking is a simple technique that involves adding a parity bit to each byte of data. The parity bit is set to either a 0 or 1 to ensure that the total number of 1 bits in the byte is even or odd.
2. **Checksum:** A checksum is a value that is calculated from the data being transmitted. The receiver calculates the checksum from the data it receives and compares it to the checksum that was transmitted with the data. If the checksums do not match, an error has occurred.
3. **Cyclic Redundancy Check (CRC):** CRC is a technique that involves adding a checksum to the data being transmitted. The receiver calculates the CRC from the data it receives and compares it to the CRC that was transmitted with the data. If the CRCs do not match, an error has occurred.

The DLC sub-layer also provides flow control through a variety of techniques. These techniques include:

1. **Stop-and-wait:**Stop-and-wait is a simple flow control technique that involves the sender transmitting a frame and then waiting for an acknowledgement from the receiver before transmitting the next frame. This technique is used when the bandwidth of the link is low or when the receiver is unable to handle a large number of frames at once.
2. **Sliding window protocol:** The sliding window protocol is a flow control technique that allows the sender to transmit multiple frames without waiting for an acknowledgement from the receiver for each frame. The sender maintains a window of frames that it has transmitted but not received an acknowledgement for. The receiver sends an acknowledgement for each frame it receives, and the sender slides the window forward as acknowledgements are received.
3. **Selective repeat protocol:** The selective repeat protocol is a flow control technique that is similar to the sliding window protocol. However, in the selective repeat protocol, the receiver can acknowledge individual frames rather than just the last frame in the window.

The DLC sub-layer also provides access control through a variety of techniques. These techniques include:

1. **Carrier Sense Multiple Access with Collision Detection (CSMA/CD):** CSMA/CD is a protocol used by Ethernet networks to control access to the physical link. CSMA/CD involves each node listening for activity on the physical link before transmitting data. If two nodes transmit data at the same time, a collision occurs, and both nodes stop transmitting and wait for a random amount of time before attempting to transmit again.
2. **Token Passing:**Token passing is a protocol used by Token Ring networks to control access to the physical link. Token passing involves a token being passed around the network, and the node that has the token is allowed to transmit data.

DISCUSSION

Data Link Control (DLC) is a sub layer of the Data Link Layer (Layer 2) in the Open Systems Interconnection (OSI) reference model. It is responsible for managing the communication between two adjacent network nodes, ensuring that data is reliably transferred between them. DLC is an important part of the network stack, as it is responsible for ensuring that data is transmitted without errors, with the correct sequence, and at the correct speed [4], [5].

DLC is responsible for taking data from the Network Layer and breaking it down into smaller, more manageable units called frames. These frames are then transmitted over the physical network.DLC must ensure that the data is transmitted without errors. To accomplish this, it adds error detection and correction codes to each frame. This ensures that if any errors occur during transmission, they can be detected and corrected.

DLC must ensure that the data is transmitted at the appropriate speed. To accomplish this, it employs flow control, which regulates the amount of data that can be sent between nodes. DLC is also responsible for controlling access to the network. It ensures that only one node can send data at a time to prevent data collisions.

This type of DLC establishes a dedicated connection between the sender and the receiver. This connection must be established before data transmission can begin. Connection-Oriented DLC is commonly used in circuit-switched networks, such as the Public Switched Telephone Network

(PSTN), where a dedicated circuit is established between the two endpoints. Connectionless DLC does not establish a dedicated connection between the sender and the receiver. Instead, each frame is sent independently and does not require an established connection. Connectionless DLC is commonly used in packet-switched networks, such as the Internet, where each packet is sent independently and can take different paths to reach its destination.

Communication in simplex mode is unidirectional, as on a one-way street. On a connection, only one of two devices can broadcast, while the other can only receive. Simplex devices include typical displays and keyboards. The monitor can only display output; the keyboard can only introduce input. Using simplex mode may transfer data in one way using the whole channel's capacity.

The half-duplex mode is comparable to a one-lane road with two-way traffic. Cars heading the opposite way must wait while those driving in one direction are moving. In a half-duplex transmission, whichever of the two devices is sending at the moment consumes the full bandwidth of a channel. Half-duplex systems are what walkie-talkies and CB (citizens band) radios use. When communication cannot take place in both ways at once and the channel's full capacity may be utilized in either direction, half-duplex mode is employed.

Full-duplex mode also known as duplex allows both stations to broadcast and receive at the same time. Similar to a two-way roadway with simultaneous traffic in both directions is the full-duplex mode. Full-duplex mode allows signals travelling in one direction to share the link's capacity with signals travelling in the opposite direction [6]. These two methods of sharing are possible: It is either necessary for the connection to have two physically distinct transmission paths one for sending, the other for receiving or the channel's capacity must be split between signals moving in both directions.

The telephone network is a typical illustration of full-duplex communication. Both parties may speak and listen at the same time while using a telephone line to communicate. When constant communication in both directions is needed, the full-duplex mode is used. Yet the channel's capacity has to be split between the two directions. A group of objects commonly referred to as nodes linked by communication connections is referred to as a network. A computer, printer, or any other device that can transmit and/or receive data produced by other nodes on the network qualifies as a node. The majority of networks use distributed processing, which divides a job across many computers. Separate computers, often a personal computer or workstation, manage a portion of a process rather than a single massive system handling all of it. A network must be able to satisfy a variety of requirements. The three that are most crucial are security, dependability, and performance.

There are several methods to gauge performance, including transit and reaction times. The length of time needed for a message to go from one device to another is known as the transit time. The period of time between a request and a response is known as the response time. The quantity of users, the kind of transmission channel, the capabilities of the linked gear, and the effectiveness of the software are some of the variables that affect how well a network performs.

Throughput and latency are two networking measures that are often used to assess performance. More throughput and reduced latency are often needed. Yet these two requirements often conflict with one another. Due to network traffic congestion, sending more data may enhance throughput, but it will also lengthen the delay. Together with delivery accuracy, network dependability is

determined by the frequency of failures, how quickly a connection recovers from a failure, and how resilient the network is to disasters. The protection of data from illegal access, the prevention of data loss and development, and the implementation of rules and processes for data recovery following breaches are all challenges related to network security.

Two or more devices linked by connections form a network. A link is a communications channel that enables the data transmission between two devices. It is easiest to visualize any connection as a line drawn between two locations for visualization reasons. Two devices must be concurrently linked to the same connection in some manner for communication to take place. Point-to-Point a dedicated link between two devices is provided through a point-to-point connection. These two devices are the only ones allowed to transmit at the full capacity of the connection. While a physical length of wire or cable is often used for point-to-point connections, alternative possibilities, including microwave or satellite links, are also a possibility.

By using an infrared remote control to change the channel on the television, you are creating a point-to-point link between the remote control and the television's control system. Multipoint A multipoint connection, also known as a multidrug connection, involves sharing a single link with more than two distinct devices. The channel's capacity is shared, either geographically or temporally, in a multipoint context. It is a spatially shared connection if many devices may utilize it at once. It is a timeshared connection if users have to switch off and on. Link b. Multipoint of a network is the geometric representation of the connections between all of the links and connecting elements (often known as nodes). There are four potential fundamental topologies: ring, bus, star, and mesh.

Mesh every device in a mesh topology has a unique point-to-point connection to every other device. According to the definition of dedicated, a connection exclusively delivers traffic between the two devices it links. We first take into account the requirement that each node be linked to every other node in order to get the total number of physical connections in a mesh network with n nodes. Node 1 must be linked to nodes in the n-I group, followed by nodes in the n-I group for node 2, and nodes in the n-I group for node n. n(n - 1) physical connections are required. On the other hand, if each physical connection supports two-way communication (duplex mode), we may divide the number of links by two. In other words, we may argue that n (n -1) /2 duplex-mode connections are required in a mesh topology. Compared to other network topologies, a mesh has a number of benefits. In the first place, using dedicated connections ensures that each connection can support its own data load, obviating the potential for traffic congestion that may arise when links are shared by many devices.

A mesh topology is also reliable. The system is not rendered useless if only one link breaks. The benefit of security or privacy comes in third. The only person who sees a message when it is sent through a dedicated line is the intended receiver. Physical restrictions prevent other users from accessing messages. Lastly, fault isolation and fault identification are made simple by point-to-point connectivity. Traffic may be rerouted to avoid connections that could have issues. This capability allows the network management to locate the issue precisely and helps in determining its source and fix [7], [8] .

The primary drawbacks of a mesh are linked to the quantity of needed cabling and I/O ports. Installation and reconnecting are challenging since every device has to be linked to every other device. Second, the wiring's sheer size may exceed the capacity of the available area (in walls, ceilings, or floors). Lastly, the hardware (I/O ports and cable) needed to connect each connection

may be unaffordable. Due to these issues, a mesh topology is often only used in restricted contexts, such as a backbone linking the central computers of a hybrid network that can support many topologies. The interconnection of telephone regional offices, where each regional office must be linked to every other regional office, is a real-world example of a mesh topology.

Skyline Topology Each device in a star topology only has a dedicated point-to-point connection to the hub, which is the central controller. There is no direct connection between the devices. A star topology does not provide direct traffic between devices, in contrast to a mesh topology. A device that wishes to communicate data to another delivers it to the controller, which then relays it to the other connected device. The cost of a star topology is lower than that of a mesh topology. Each device in a star only requires one connection and one I/O port to connect to any number of other devices. It is also simple to install and adjust due to this aspect. The hub and that device only need to be connected for additions, moves, and deletions, thus much less wiring has to be stored. Robustness is one of the benefits. Just one connection is impacted if it fails. The other links are still live. This component also makes it simple to identify faults and

The hub may be used to track link issues and avoid broken links as long as it is operational. The dependence of a star topology on a single point, the hub, is one of its major drawbacks. The system is dead if the hub malfunctions. A star needs far less wire than a mesh, but each node still has to be connected to the main hub. Because of this, a star topology often requires more cabling than some other designs (such as ring or bus). Bus Topography All of the aforementioned instances are of point-to-point connections. On the other hand, a bus topology is multipoint. The backbone of a network is made up of one lengthy wire that connects all the devices.

Drop lines and taps are used to connect nodes to the bus wire. A connection between the gadget and the main cable is known as a drop line. A tap is a connector that makes a connection with the metallic core of a cable by either splicing into the main cable or cutting through the cable's wrapping. Some of the energy of a signal is converted into heat as it moves through the backbone. As a result, as it moves further and farther, it becomes weaker and weaker. Because of this, there are restrictions on the quantity of taps and the spacing between them that a bus can sustain.

A bus topology has the benefit of being simple to implement. The most effective route for laying backbone cable may be chosen, and drop lines of different lengths can be used to link it to the nodes. A bus requires less cabling than a mesh or star topology in this manner. For instance, in a star, four network devices in the same room need four lengths of wire to reach the hub this redundancy is removed in a bus. Just the backbone wire traverses the whole construction. Each drop line simply has to extend as far as the spine's closest point [9], [10].

Inconvenient reconnecting and fault separation are two drawbacks. Typically, a bus is built to be installed as efficiently as possible. So, adding more devices may be challenging. Quality reduction may result from signal reflection at the taps. Limiting the quantity and proximity of devices connected to a particular length of wire will prevent this deterioration. The backbone could consequently need to be changed or replaced in order to accommodate additional devices.

However, even communication between devices on the same side of the issue is halted by a failure or break in the bus cable. Noise is produced in both directions as a result of the damaged region reflecting signals back in the direction of origin. One of the earliest topologies utilized in the creation of early local-area networks was the bus topology. Bus topologies may be used in

Ethernet LANs, although they are less common nowadays for reasons that we shall cover. Topology of rings each device in a ring topology has a unique point-to-point connection, with only the other two devices on each side. From one device to the next, along the ring, a signal is sent in a single direction until it reaches its target. Each component of the ring contains a repeater. A device's repeater regenerates the bits and sends them on when it receives a signal meant for another device.

Installing and rearranging a ring is not that difficult. Just the devices that are right next to one other are connected either physically or logically. Adding or removing a device simply needs two connections to be changed. The only limitations are those related to the media and traffic maximum ring length and number of devices. Fault isolation is also made simpler. In a ring, a signal typically circulates constantly. One gadget has the ability to sound an alert if it doesn't get a signal within a certain time frame. The alarm notifies the network administrator of the issue's existence and location. Unidirectional traffic, however, may have drawbacks. A break in the ring (such as a disabled station) may bring down the whole network in a basic ring. The use of a dual ring or a switch that can shut off the break will address this vulnerability. When IBM released its local-area network Token Ring, ring topologies were common. Currently, this architecture is less common due to the need for faster LANs. Combined Topology Hybrid networks are possible we may, for instance, have a primary star topology with each branch linking many stations.

Different entities build computer networks. These diverse networks can’t connect with one another without standards. The OSI model and the Internet model are the two most well-known standards. The Internet model specifies a five-layer network, but the OSI (Open Systems Interconnection) model defines a seven-layer network. Although sporadic allusions to the OSI model, this book is mostly based on the Internet model. Currently, local-area networks and wide-area networks are the two main types of networks that are often mentioned. A network’s size determines which category it belongs in. A WAN may be global, but a LAN typically covers an area of less than 2 km. Middle-sized networks, which often cover tens of miles, are known as metropolitan area networks.

The devices in a single workplace, building, or campus are connected by a local area network (LAN), which is often privately owned. A LAN may be as basic as two PCs and a printer in someone’s home office, or it might stretch across an entire corporation and include audio and video peripherals, depending on the demands of an organization and the sort of technology utilized. LAN size is currently restricted to a few kilometers. Resources may be exchanged across workstations or personal computers thanks to local area networks (LANs). Hardware (such as a printer), software (such as an application programme), or data are just a few examples of the resources that may be shared. A typical LAN example is a workgroup of task-related computers, such as engineering workstations or accounting PCs that are connected in many company situations. In order to service customers, one of the PCs can get a large-capacity disc drive. On this central server, software may be kept and utilised as required by the whole team. In this example, licencing constraints on the number of users per copy of software or limits on the number of users permitted to access the operating system may dictate the size of the Network. LANs are differentiated from other kinds of networks in addition to size by their transmission medium and topology. A particular LAN will typically only use one kind of transmission media. The bus, ring, and star LAN topologies are the most popular.

A wide area network (WAN) enables long-distance data, picture, audio, and video transmission over expansive geographic regions, which may include a whole nation, a continent, or even the entire planet. We go into further information about wide-area networks. A wide area network (WAN) may be as intricate as the backbones that link the Internet or as simple as a dial-up connection connecting a home computer to the Internet. The first is often referred to as a switched WAN, while the second is referred to as a point-to-point WAN [11]. The end systems are connected via the switched WAN, which is often a router an internetworking connecting device that is connected to another LAN or WAN. The point-to-point WAN links a home computer or small LAN to an Internet service provider often using a line leased from a telephone or cable TV provider (lSP). Access to the Internet is often provided using this kind of WAN.

CONCLUSION

Data Link Control (DLC) is a sub layer of the Data Link layer in the OSI network model, responsible for establishing, maintaining, and terminating logical connections between two communicating devices, and ensuring the reliable transfer of data over the physical layer. Data Link Control is essential for ensuring the efficient and reliable transfer of data over a network. It provides a set of procedures, protocols, and standards that enable data transmission, error detection, correction, and flow control. It also helps in managing the access of multiple devices to the network and preventing data collisions. Overall, DLC plays a critical role in the effective functioning of a network, and its importance cannot be overstated.

REFERENCES

[1] W. Feng, Y. Li, X. Yang, Z. Yan, and L. Chen, “Blockchain-based data transmission control for Tactical Data Link,” *Digit. Commun. Networks*, 2021, doi: 10.1016/j.dcan.2020.05.007.

[2] M. Lv, H. Huang, and X. Li, “An Ethernet Mapping High-Level Data Link Control Circuit Design,” in *Lecture Notes on Data Engineering and Communications Technologies*, 2022. doi: 10.1007/978-3-030-89698-0_122.

[3] K. S. Chan, S. Chan, and K. T. Ko, “A data link control protocol for broadband wireless networks with adaptive coding rate,” *Int. J. Commun. Syst.*, 2006, doi: 10.1002/dac.769.

[4] W. Bux, K. Kümmerle, and H. L. Truong, “Data link-control performance: Results comparing HDLC operational modes,” *Comput. Networks*, 1982, doi: 10.1016/0376-5075(82)90121-0.

[5] A. S. A. Varma, “Data Link Control in Data Communication,” *IOSR J. Electron. Commun. Eng.*, 2012, doi: 10.9790/2834-0413947.

[6] H. Kim, S. K. Biswas, P. Narasimhan, R. Siracusa, and C. Johnston, “Design and implementation of a QoS oriented data-link control protocol for CBR traffic in wireless ATM networks,” *Wirel. Networks*, 2001, doi: 10.1023/A:1016778728006.

[7] D. E. Carlson, “Bit-Oriented Data Link Control Procedures,” *IEEE Trans. Commun.*, 1980, doi: 10.1109/TCOM.1980.1094692.

[8] M. Lott, R. Halfmann, E. Schulz, M. Meincke, M. D. Perez Guirao, and K. Jobmann, “Data link control,” in *Inter-Vehicle-Communications Based on Ad Hoc Networking*

Principles: The FleetNet Project, 2005. doi: 10.5445/KSP/1000003684.

[9] G. A. Aderounmu, E. R. Adagunodo, and A. D. Akinde, "Performance comparison of data-link control protocol for wireless asynchronous transfer mode network," *Int. J. Comput. Appl.*, 2002, doi: 10.1080/1206212X.2002.11441674.

[10] R. A. Donnan and J. R. Kersey, "SYNCHRONOUS DATA LINK CONTROL: A PERSPECTIVE.," *IBM Syst. J.*, 1974, doi: 10.1147/sj.132.0140.

[11] C. Ward, C. H. Choi, and T. F. Hain, "A Data Link Control Protocol for LEO Satellite Networks Providing a Reliable Datagram Service," *IEEE/ACM Trans. Netw.*, 1995, doi: 10.1109/90.365441.

CHAPTER 18

PERFORMANCE EVALUATION OF DATA LINK CONTROL PROTOCOLS FOR EFFICIENT DATA TRANSFER IN COMMUNICATION NETWORKS

Prashant Kumar, Assistant Professor
Department of Electronics and Communication Engineering,
Teerthanker Mahaveer University, Moradabad, Uttar Pradesh, India
Email Id- tmu.iqac@gmail.com

ABSTRACT:

Data Link Control (DLC) protocols are a set of rules and procedures used to ensure the reliable transfer of data between two devices over a communication network. These protocols are implemented at the Data Link layer of the OSI model and are responsible for establishing, maintaining, and terminating logical connections between devices. DLC protocols provide a range of functions such as framing, error detection and correction, flow control, and data synchronization. They also help in managing access to the network and preventing data collisions. Some commonly used DLC protocols include High-Level Data Link Control (HDLC), Point-to-Point Protocol (PPP), and Serial Line Internet Protocol (SLIP).

KEYWORDS:

Communication Network, Data Link Control, Error Detection, Serial Line, Point to Point Protocol.

INTRODUCTION

Data link control and media access control are the two major duties of the data link layer. The first, data link control, deals with the plans and methods for node-to-node communication between two nearby nodes. This chapter includes a discussion of this feature. Media access is the data connection layer's second purpose [1], [2]. Framing, flow control, and software-implemented protocols all play a part in the seamless and reliable delivery of frames between nodes during data link control operations. Organizing the bits that are carried by the physical layer is referred to as framing, and it is the first topic we cover in this chapter. Next, we talk about flow and error handling. Techniques for error detection and correction, a subset of this subject.

We need methods to put data link control into practice. Each protocol consists of a set of instructions that must be carried out by the two nodes engaged in data exchange at the data connection layer. Five procedures are covered: two for ideal (noiseless) channels and three for noisy (actual) channels. While the first category's protocols are not in use, they serve as a starting point for comprehending the second category's protocols [3]. After addressing the five protocol concepts, we use the High-level Data Link Control (HDLC) Protocol as an example to demonstrate how a bit-oriented protocol is really put into practice. We also go through the Point-to-Point Protocol, a well-liked byte-oriented protocol (PPP).

Moving bits in the form of a signal from the source to the destination is what is meant by data transmission in the physical layer. To make sure that the transmitter and receiver utilize the same

bit durations and timing, the physical layer offers bit synchronization. In contrast, the data connection layer must cram bits into frames such that they can be distinguished from one another. Our postal service engages in a kind of framing[4], [5]. One piece of information is separated from another by the simple act of sealing a letter inside an envelope; the envelope acts as the delimiter. As the postal system is a many-to-many carrier service, the sender and recipient addresses are also included on each envelope. By including a sender address and a destination address, framing at the data connection layer divides a message from one source to a destination or from other messages to other destinations. The sender address assists the receiver in acknowledging receipt while the destination address specifies where the packet is to travel.

While the whole message may fit in one frame, it is not customary to do so. One explanation is that a frame may be rather big, which would make flow and error control quite ineffective. Even a single bit mistake would need retransmission of the whole message when a message is transmitted in a single, extremely big frame. A single-bit mistake only affects that particular little frame when a message is broken up into smaller frames.

Frame sizes may be either fixed or variable. The borders of the frames don't need to be specified when using fixed-size framing; the size itself might act as a delimiter. The ATM wide-area network, which employs frames of a defined size called cells, serves as an illustration of this framing style. In Chapter 18, we go through ATM.

This chapter's major focus is on the common practise of variable-size framing in local-area networks. We need a method to specify the conclusion of one frame and the start of the next in variable-size framing. Both a character-oriented approach and a bit-oriented approach have historically been utilised for this purpose.

Data to be carried in a character-oriented protocol are 8-bit characters from an ASCII coding scheme (see Appendix A). Both the header, which often contains the source and destination addresses as well as other control information, and the trailer, which typically contains redundant bits for error detection or error correction, are multiples of 8. An 8-bit (I-byte) flag is inserted at the start and end of a frame to distinguish it from the next frame [6]. The flag, which is made up of protocol-specific special characters, indicates whether a frame is beginning or ending.

Since the data connection layers were merely exchanging text, character-oriented framing was widely used. The flag might be any character not often used for text messaging. But, we now provide more sorts of data, including graphs, audio, and video. Any design used for the flag might potentially be a component of the data. If this occurs, the receiver will mistakenly believe that it has reached the end of the frame when it meets this pattern in the midst of the data. A byte-stuffing technique was introduced to character-oriented framing address this issue. When a character matches the flag's pattern, byte stuffing (also known as character stuffing) adds a specific byte to the frame's data section. There is an additional byte in the data area. The escape character (ESC), which is the name given to this byte, has a predetermined bit sequence. When the ESC character appears, the receiver removes it from the data section and uses the following character as data rather than a delimiting indicator.

DISCUSSION

The existence of the flag in the data portion of the frame is made possible by byte stuffing by the escape character, however this leads to another issue. What happens if the text has a flag and one

or more escape characters? The escape character is removed by the receiver, but the flag is retained and mistakenly considered to be the end of the frame [7], [8]. This issue may be fixed by marking the escape characters that are already present in the text with an additional escape character. In other words, if the escape character already exists in the text, another one will be inserted to indicate that the second escape character already exists in the text. The 16-bit and 32-bit characters of today's universal coding schemes, such Unicode, clash with the 8-bit characters. Overall, we can conclude that the trend is towards the bit-oriented protocols that we will cover next.

In a bit-oriented protocol, a frame's data portion consists of a series of bits that the top layer will decode into text, graphics, audio, video, and other types of data. To distinguish one frame from the next, we still need a delimiter in addition to headers (and maybe trailers). Most protocols employ a specific 8-bit pattern indicator called a delimiter to indicate the start and end of a frame, 01111110. At least two devices must cooperate in order for data to be sent; one must send data while the other receives it. Even with such a simple setup, it takes a lot of coordination to have a meaningful conversation. Flow control and error control are the data connection layer's two most significant duties. Data link control is the term for these activities taken together.

One of the most significant responsibilities of the data connection layer is the coordination of flow control, which regulates the amount of data that may be transferred before receiving an acknowledgement. In the majority of protocols, flow control refers to a sequence of steps that specify how much data may be sent before the recipient must acknowledge it. The receiver must not be overloaded by the data flow. Each receiving device has a maximum processing speed for incoming data and a maximum memory capacity for storing incoming data. Before certain thresholds are reached, the receiving device must be able to alert the sending device and make a request for it to send fewer frames or temporarily halt transmission.

Before being utilized, incoming data must be verified and processed. Often, the processing speed takes longer than the transmission speed. Because of this, each receiving device has a memory space designated as a buffer where incoming data are stored until processing begins. Receiving a signal if the buffer starts to fill up Let's now examine how data delivery from one node to another may be accomplished using the data connection layer's integration of framing, flow control, and error control. A standard programming language is often used to implement the protocols in software. We have constructed a version of each protocol in pseudo code that focuses mostly on the process rather than going into the specifics of language rules.

The protocols that can be used for noiseless (error-free) channels and those that can be used for noisy (error-creating) channels are discussed separately. While the first group of protocols cannot be used in practice, they provide a framework for understanding the protocols of noisy channels. The protocols we describe here and those utilized in actual networks are not the same. In that the data frames go from one node, known as the sender, to another node, known as the receiver, all the protocols we examine are unidirectional. Data only flows in one way, despite the fact that special frames such as acknowledgement (ACK) and negative acknowledgment (NAK) may travel in the other direction to aid with flow and error management. The data connection protocols used in actual networks are bidirectional, allowing data to flow in both ways. The flow and error control information, such as ACKs and NAKs, is piggybacked onto the data frames in these protocols.

We picked unidirectional protocols for our explanation since bidirectional ones are more complicated. They can be used to bidirectional protocols if they are understood. This expansion is left as an exercise. Assume for the moment that we have a perfect channel with no frames being lost, duplicated, or corrupted. Two protocols are shown here for this kind of channel. The first approach does not use flow control, whereas the second does. We have presumptively assumed that the channel is a perfect noiseless channel, therefore of course neither has error control.

For lack of a better word, we refer to our initial protocol, the Simplest Protocol, as having no flow or en'or control. It is a unidirectional protocol, like the other ones we'll cover in this chapter, meaning that data frames may only go in one direction: from sender to receiver. We assume that each frame the receiver gets may be handled instantly with a processing time that is trivial in size. The information layer of As soon as possible, the receiver takes off the header from the frame and gives the data packet to its network layer, which may also accept it right away. To put it another way, the receiver can never receive too many incoming frames.

With this method, flow control is not required. The sender site's data connection layer receives data from its network layer, frames the data, and transfers it. The receiver site's data connection layer gets a frame from its physical layer, takes the frame's data out of it, and sends the data to its network layer. The sender's and receiver's data connection layers provide transmission services for their respective network levels. The physical transfer of bits is handled by the data link levels using the services offered by respective physical layers signaling, multiplexing, etc.. We must go into more detail about how both data link layers operate. Until the network layer of the sender site has a data packet to deliver, it cannot send a frame.

Until a frame arrives, the receiver site cannot transfer a data packet to its network layer. We must add the concept of events in the protocol if it is implemented as a process. The process is operating continuously at the sender site; nothing happens until the network layer initiates a request. The process is running continuously at the receiver location as well, but nothing is done until the physical layer sends a notice. Due of the uncertainty around the timing of the related occurrences, both processes are always in operation. Analysis Because of the algorithm's endless loop, lines 3 through 9 are repeated indefinitely after the programme starts. Since the algorithm is event-driven, it sleeps (line 3) until an event causes it to wake up (line 4). This indicates that there is a pause between the execution of lines 3 and 4 and that the amount of time between them may not be known. Lines 6 through 8 are performed when the event, a network layer request, takes place. The loop is then repeated, and the programmed sleeps at line 3 once again until the next time the event occurs. For the primary step, we have created pseudo code. With the modules Get Data, Data frames must be kept until use if they arrive at the receiver location quicker than they can be processed. The receiver often lacks sufficient store capacity, particularly if it is receiving data from several sources. Denial of service or the discarding of frames might happen as a consequence. We need to find a way to signal the transmitter to slow down so the receiver isn't overloaded with frames. Feedback from the recipient to the sender is required.

The protocol we'll be discussing right now is known as the Stop-and-Wait Protocol because after sending a frame, the sender waits for the receiver to indicate that it is alright to go on before sending the next frame. Data frames still flow in a single path, but supplemental ACK frames—simple signals of acknowledgment travel in the other way. We extend our earlier technique with flow control. Error detection is a practical method that may be found in transport protocols like

TCP and data link control protocols like HDLC. Yet, a block of data must be retransmitted in order to repair faults using an error-detecting algorithm.

The system that results is incredibly ineffective. Retransmitting the frame in mistake together with all succeeding frames is the standard method. Instead, it would be preferable to provide the receiver the ability to fix transmission mistakes based on the bits included in the message. Each k-bit block of data is sent as Ai P1X2 = g A0 = An-k = 1 n-k i=0. K pieces of AiXi. The CRC register is often seen moving to the right, the opposite of the parallel to binary division. The most important bit in binary integers is often shown on the left, therefore using a left-shifting register, as is done here, is preferable. The signal is susceptible to impairments during transmission, which might result in bit mistakes in the signal. The incoming signal is demodulated at the receiver to create a bit string that resembles the original code word but may include mistakes.

How may bit mistakes be corrected by the decoder? In essence, redundancy is added to the transmitted message as part of error correction. Even in the presence of a certain amount of error rate, the redundancy enables the receiver to determine what the original message was. This section examines block error-correcting code, a popular kind of error-correcting code. Our discussion is limited to fundamental ideas; we do not address particular error-correcting codes in detail. Before moving on, it should be noted that the error-correcting code often has the same basic structure as the error-detecting code depicted. In other words, the FEC algorithm takes a k-bit block as input and adds check bits to it to create an n-bit block, with all of the bits from the original k-bit block present. In certain FEC algorithms, the k-bit input is translated into an n-bit code word in a manner that prevents the original k bits from showing up in the code word.

The number of bits in which two n-bit binary sequences and differ is known as the Hamming distance. For instance, if, then let's now think about the block coding method of mistake correction. Let's say we want to send k-bit-long data chunks across the internet. We translate each k-bit sequence into a distinct n-bit code word rather than sending each block ask bits d1v1, v22 = 3 v1 = 011011, v2 = 110001, v2 v1 v2 v1, and 1n - k2 1n 7 k2, respectively. The receiver has identified a mistake since this is an invalid code word. Can the mistake be fixed? Since one, two, three, four, or even all five of the bits that were communicated may have been tainted by noise, we cannot be certain which data block was delivered. However note that the legal code word 00000 might be changed to 00100 with only one bit change. 00111 to 00100 would require two bit changes, 11110 to 00100 would require three bit changes, and 11001 to 00100 would require four bit changes. We can therefore conclude that the desired data block is 00 and that the most likely code word that was sent was 00000.

The aforementioned example highlights the key characteristics of a block error-correcting code. K data bits are converted into n-bit code words using a (n, k) block code. Typically, to create an n-bit code word, each valid code word copies the original k data bits and check bits to them. Therefore, the creation of a block code is equivalent to the creation of a function of the form where and are vectors of k data bits and n code word bits, respectively. Out of all possible code words, there are valid code words with a (n, k) block code. The redundancy of the code is measured as the ratio of redundant bits to data bits, and the code rate is measured as the ratio of data bits to total bits, or k/n. The code rate is a measurement of the additional bandwidth needed to transmit data at the same rate as before the code was present. For instance, to maintain the same data rate with a code rate of 1/2, the transmission capacity of an encoded system must be doubled. Since the code rate in our example is 2/5, an encoded system needs 2.5 times as much

space. For instance, the encoder must output data at a rate of 2.5 Mbps in order to keep up with a data rate input of 1 Mbps.

As a result, if such an invalid codeword is received, it may have been the result of a 2 bit error, leaving the receiver unable to choose between the two possibilities. Although an error is discovered, it cannot be fixed. However, every time a single bit error happens, the resulting codeword is only 1 away from being a valid codeword, allowing the choice to be made. Therefore, this code can fix any single-bit error, but it cannot fix double-bit errors. Looking at the pairwise distances between valid codewords is another way to see this. A minimum of three words must separate each valid codeword. Therefore, a single bit error will result in an invalid codeword that is a distance 1 from the original valid codeword but a distance at least 2 from all other valid codewords. As a result, the code can always correct a single-bit error. Note that the code also will always detect a double-bit error.

It can be shown that the following conditions hold. For a given positive integer t, if a code satisfies then the code can correct all bit errors up to and including errors of t bits. If then all bits can be corrected and errors of t bits can be detected but not, in general, corrected. Conversely, any code for which all errors of are corrected must satisfy and any code for which all errors of are corrected and all errors of magnitude t are detected must satisfy. Another way of putting the relationship between and t is to say that the maximum number of guaranteed correctable errors per codeword satisfies where means the largest integer not to exceed x (e.g.,). (e.g.,). Furthermore, if we are concerned only with error detection and not error correction, then the number of errors that can be detected satisfies

The literature on error-correcting codes frequently includes graphs of this sort to demonstrate the effectiveness of various encoding schemes. Curve on the right is for an uncoded modulation system; the shaded region represents the area in which improvement can be achieved. In this region, a smaller BER (bit error rate) is achieved for a given and conversely, for a given BER, \sa smaller is required. The other curve is a typical result of a code rate of onehalf (equal number of data and check bits) (equal number of data and check bits). It is important to realise that the BER for the second rate 1/2 curve refers to the rate of uncorrected errors and that the value refers to the energy per data bit.

Because the rate is 1/2, there are two bits on the channel for each data bit, and the energy per coded bit is half that of the energy per data bit, or a reduction of 3 dB to a value of 8 dB. If we look at the energy per coded bit for this system, then we see that the channel bit error rate is about or 0.024. Finally, note that below a certain threshold of, the coding scheme actually degrades performance. Below the threshold, the extra check bits add overhead to the system that reduces the energy per data bit causing increased errors. Above the threshold, he error-correcting power of the code more than compensates for the reduced, resulting in a coding gain. Two characteristics that distinguish various data link configurations are topology and whether the link is half duplex or full duplex.

Traditional multipoint topologies are made possible when the terminals are only transmitting a fraction of the time. If each terminal has a point-to-point link to its computer, then the computer must have one I/O port for each terminal. Also there is a separate transmission line from the computer to each terminal. In a multipoint configuration, the computer needs only a single I/O port and a single transmission line, which saves costs. Data exchanges over a transmission line can be classified as full duplex or half duplex. With half-duplex transmission, only one of two

stations on a point-to-point link may transmit at a time. This mode is also referred to as two-way alternate, suggestive of the fact that two stations must alternate in transmitting. This can be for full-duplex transmission, two stations can simultaneously send and receive data from each other. Thus, this mode is known as two-way simultaneous and may be compared to a two-lane, two-way bridge. For computer-to-computer data exchange, this form of transmission is more efficient than half-duplex transmission [9].

With digital signalling, which requires guided transmission, full-duplex operation usually requires two separate transmission paths (e.g., two twisted pairs), while half duplex requires only one. For analogue signalling, it depends on frequency: If a station transmits and receives on the same frequency, it must operate in half-duplex mode for wireless transmission, although it may operate in full-duplex mode for guided transmission using two separate transmission lines. If a station transmits on \sone frequency and receives on another, it may operate in full-duplex mode for wireless transmission and in full-duplex mode with a single line for guided transmission. It is possible to transmit digital signals simultaneously in both directions on a single transmission line using a technique called echo cancellation. This is a signal processing technique whose explanation is beyond the scope of this book. The Stop-and-Wait Protocol provides us a concept of how to extend its predecessor with flow control, but noiseless channels do not exist. Either we need to add error control to our protocols or we may choose to disregard the error like we sometimes do. In this part, we cover three error-controlling methods.

The Stop-and-Wait Automatic Repeat Request (Stop-andWait ARQ), our first protocol, extends the Stop-and-Wait Protocol with a basic error control mechanism. Let's check out how this protocol identifies and fixes faults. Redundancy bits must be added to our data frame in order to identify and fix faulty frames. The frame is examined when it reaches the receiver site, and if it is corrupted, it is quietly discarded. The receiver's silence indicates that there are faults in this protocol. Corrupted frames are easier to manage than lost ones. Prior to this, there was no method to recognise a frame in our procedures. The frame that was received may be the right one, a duplicate, or a frame that was out of sequence. The frames should be numbered as a solution. A data frame that the receiver gets out of order indicates that one or more frames were lost or duplicated.With this protocol, the completed and missing frames must be transmitted again. How can the sender determine which frame to resend if the recipient doesn't acknowledge an issue when it occurs? The sender saves a copy of the transmitted frame as a workaround for this issue. It also begins a timer at the same time. The frame is sent again, the copy is kept, and the countdown is repeated if the timer ends and there is no ACK for the transmitted frame. Even though there may be several copies of a frame on the network due to the protocol's stop-and-wait mechanism, only one particular frame requires an ACK. In Stop-and-Wait ARQ, error correction is accomplished by saving a copy of the delivered frame and retransmitting the frame after the timer ends. An ACK frame also requires redundancy bits and a sequence number since it is susceptible to corruption and loss. With this protocol, a sequence number field is included in the ACK frame.

With this protocol, a malformed or out-of-order ACK packet is simply ignored by the sender. The protocol mandates that frames must be numbered, as we previously described. Using sequence numbers allows for this. The data frame gains a field to store the frame's sequence number. The range of the sequence numbers is one significant factor to take into account. In order to reduce the size of the frame, we search for the lowest range that offers unambiguous[10], [11].The sequence numbers may wrap. For instance, if the field is determined

to be m bits long, the sequence numbers begin at 0 and proceed up to 2m – 1 before being repeated. Let's determine the range of sequence numbers we need using logic. If we've already used x as a sequence number, the next number we need to utilise is x + 1. x + 2 is not required. Assume that the sender delivered frame number x to demonstrate this. Three things are possible.

1. The frame is sent to the recipient site safely, and the recipient provides a confirmation. When the acknowledgement reaches the sender site, the sender sends the frame with the number x + 1 as the following frame.
2. The frame reaches the receiver site safely; however, the acknowledgement that the receiver sends is lost or distorted. After the time-out, the sender transmits the frame (numbered x) again. The frame in this instance is a duplication. The receiver can detect this as it was expecting frame x + I but only got frame x.
3. The frame is damaged or never reaches the recipient site; after the time-out, the sender resends the frame (numbered x).

CONCLUSION

Data Link Control (DLC) protocols are a set of procedures and standards that ensure the reliable transfer of data over a communication network. DLC protocols are implemented at the Data Link layer of the OSI model and provide functions such as framing, error detection and correction, flow control, and data synchronization. DLC protocols are critical for ensuring efficient and reliable communication between devices in a network. They enable data to be transmitted accurately and securely and help prevent data collisions and network congestion. Some widely used DLC protocols include HDLC, PPP, and SLIP, which are used in various applications such as X.25, ISDN, and Frame Relay.

REFERENCES

[1] W. Feng, Y. Li, X. Yang, Z. Yan, and L. Chen, “Blockchain-based data transmission control for Tactical Data Link,” *Digit. Commun. Networks*, 2021, doi: 10.1016/j.dcan.2020.05.007.

[2] M. Lv, H. Huang, and X. Li, “An Ethernet Mapping High-Level Data Link Control Circuit Design,” in *Lecture Notes on Data Engineering and Communications Technologies*, 2022. doi: 10.1007/978-3-030-89698-0_122.

[3] K. S. Chan, S. Chan, and K. T. Ko, “A data link control protocol for broadband wireless networks with adaptive coding rate,” *Int. J. Commun. Syst.*, 2006, doi: 10.1002/dac.769.

[4] W. Bux, K. Kümmerle, and H. L. Truong, “Data link-control performance: Results comparing HDLC operational modes,” *Comput. Networks*, 1982, doi: 10.1016/0376-5075(82)90121-0.

[5] A. S. A. Varma, “Data Link Control in Data Communication,” *IOSR J. Electron. Commun. Eng.*, 2012, doi: 10.9790/2834-0413947.

[6] H. Kim, S. K. Biswas, P. Narasimhan, R. Siracusa, and C. Johnston, “Design and implementation of a QoS oriented data-link control protocol for CBR traffic in wireless ATM networks,” *Wirel. Networks*, 2001, doi: 10.1023/A:1016778728006.

[7] D. E. Carlson, “Bit-Oriented Data Link Control Procedures,” *IEEE Trans. Commun.*, 1980, doi: 10.1109/TCOM.1980.1094692.

[8] M. Lott, R. Halfmann, E. Schulz, M. Meincke, M. D. Perez Guirao, and K. Jobmann, "Data link control," in *Inter-Vehicle-Communications Based on Ad Hoc Networking Principles: The FleetNet Project*, 2005. doi: 10.5445/KSP/1000003684.

[9] G. A. Aderounmu, E. R. Adagunodo, and A. D. Akinde, "Performance comparison of data-link control protocol for wireless asynchronous transfer mode network," *Int. J. Comput. Appl.*, 2002, doi: 10.1080/1206212X.2002.11441674.

[10] R. A. Donnan and J. R. Kersey, "SYNCHRONOUS DATA LINK CONTROL: A PERSPECTIVE.," *IBM Syst. J.*, 1974, doi: 10.1147/sj.132.0140.

[11] C. Ward, C. H. Choi, and T. F. Hain, "A Data Link Control Protocol for LEO Satellite Networks Providing a Reliable Datagram Service," *IEEE/ACM Trans. Netw.*, 1995, doi: 10.1109/90.365441.

CHAPTER 19

DESIGN AND IMPLEMENTATION OF A ROBUST DATA LINK CONTROL PROTOCOL FOR HIGH-SPEED COMMUNICATION NETWORKS

Rahul Vishnoi, Assistant Professor
Department of Electronics and Communication Engineering,
Teerthanker Mahaveer University, Moradabad, Uttar Pradesh, India
Email Id- ra_v@yahoo.com

ABSTRACT:

Data Link Control (DLC) protocols are a set of standards and procedures used to ensure efficient and reliable data transfer between two devices over a communication network. These protocols are implemented at the Data Link layer of the OSI model and provide a range of functions such as error detection and correction, flow control, and data synchronization. DLC protocols are essential for establishing and maintaining logical connections between devices and preventing data collisions. They help in the effective transmission of data across a network and ensure that data is delivered accurately and securely.

KEYWORDS:

Communication Network, Data Link Control, Data Synchronization, Protocols, Flow Control.

INTRODUCTION

Before we learn anything about the preceding frames, a number of frames may be transmitted. If there are many bits in transition relative to the bandwidth-delay product, pipelining increases transmission efficiency. Several frames must be in transition while waiting for acknowledgement to increase transmission efficiency (fill the pipe). In order to keep the channel active while the sender waits for acknowledgement, we must allow more than one frame to remain outstanding. We go over one procedure that can help us accomplish this aim in this part, and we go over another in the one after [1]–[4].

The first is known as Go-Back-N Automatic Repeat Request; its meaning will be made evident in a moment. Using this protocol, we may transmit several frames without getting acknowledgements; we store copies of these frames until we do. A transmitting station's frames are consecutively numbered.

But, we must establish a cap since the header must include the sequence number of each frame. Sequence numbers may vary from 0 to 2m - 1 if the frame's header permits m bits for the sequence number. The only sequence numbers are 0 through 15 inclusive, for instance, if m equals 4. The sequence numbers are modulo-2m, in other words.

The sequence numbers in the Go-Back-N Protocol are modulo 1, where m is the bit size of the sequence number field. The sliding window in this protocol and the one after it refers to the range of sequence numbers that the sender and receiver are interested in. In other words, just a portion of the available sequence numbers must be handled by the sender and recipient. The

range that the transmitter is concerned with is referred to as the send sliding window, and the range that the receiver is concerned with is referred as receive sliding window. Here, we talk about both.

The transmit window is a hypothetical box that includes the potential transiting data frames' sequence numbers. Some of these sequence numbers specify the frames that have already been transmitted in each window location, while others specify the frames that may still be sent. For reasons we'll go into later, the window can only be a maximum of 2m - 1. We set the size to its maximum value and left it constant for the sake of this chapter, but we'll learn in later chapters that certain protocols may have changeable window sizes.

Send window after sliding frames with already acknowledged sliding numbers. The sender is unconcerned with these frames and does not retain any copies of them. The range of sequence numbers that are associated with the transmitted frames that have an uncertain status is defined by the second area. The sender must wait to see if these frames were received or not. We refer to these frames as outstanding. Since the relevant data packets have not yet been received from the network layer, the third range, shown in white in the picture, specifies the range of sequence numbers for frames that may be delivered. The fourth area, which we'll get to later, specifies sequence numbers that are reserved for use only after the window moves.

Three factors determine the size and placement of the window at any one moment; the window itself is an abstraction. Sf (send window, the first outstanding frame), Sn (send window, the next frame to be sent), and Size are the names of these variables (send window, size). The first (oldest) outstanding frame's sequence number is indicated by the variable Sf. The sequence number that will be allocated to the next frame to be transmitted is stored in the variable Sn. The size of the window is lastly defined by the variable Size, which is fixed in our protocol [5].

As we shall see in a moment, this protocol's acknowledgments are cumulative, thus each ACK packet may acknowledge many frames, and the window has moved three slots to the right. Since frame 3 is now the only unfinished frame, it should be noted that the value ofSf is 3. The relevant data frames are received and the appropriate acknowledgments are issued thanks to the receive window. The receive window's size is always I. The receiver is always watching for the entry of a certain frame [6].

Notice that to create this abstraction, we just need the single variable Rn (receiving window, next frame anticipated). The frames that have previously been received and acknowledged are identified by the sequence numbers to the left of the window, while the frames that can't be received are identified by the sequence numbers to the right of the window. Any received frame that has a sequence number in any of these two areas is ignored. The only frames that are recognised and acknowledged are those whose sequence numbers match the value of Rn. Just one slot slides at a time in the receiving window, which likewise slides. The window moves when a proper frame is received and only one frame is received at a time. Despite the fact that there might be a timer for each frame delivered, our protocol only uses one. Since the timer for the first unsent frame always runs out first, we transmit all pending frames as soon as it does [7].

DISCUSSION

If a frame arrives intact, safe, and in good condition, the receiver provides a positive acknowledgement. The receiver remains quiet and discards all following frames until it gets the

expected frame if a frame is destroyed or received out of sequence. The transmitter resends all pending frames when the timeout expires. Consider a scenario in which the sender has already transmitted frame 6 but frame 3's timer has already run out. The sender then transmits frames 3, 4,5, and 6 once again since frame 3 has not been acknowledged. The protocol is known as Go-Back-N ARQ for this reason. As we can see, several frames may be moving ahead and numerous acknowledgments may be moving backward. The concept is comparable to Stop-and-Wait ARQ; however, the transmit

Because of the possibility of transmission errors, and because the receiver of data may need to regulate the rate at which data arrive, synchronization and interfacing techniques are insufficient by themselves. It is necessary to impose a layer of control in each communicating device. Flow control enables a receiver to regulate the flow of data from a sender so that the receiver's buffers do not overflow.In a data link control protocol, error control is achieved by retransmission of damaged frames that have not been acknowledged or for which the other side requests a retransmission.High-level data link control (HDLC) is a widely used data link control protocol. It contains virtually all of the features found in other data link control protocols.

Our discussion so far has concerned sending signals over a transmission link. For effective digital data communications, much more is needed to control and manage the exchange. In this chapter, we shift our emphasis to that of sending data over a data communications link. To achieve the necessary control, a layer of logic is added above the physical layer discussed in Chapter 6; this logic is referred to as data link control or a data link control protocol. When a data link control protocol is used, the transmission medium between systems is referred to as a data link. Link management: The initiation, maintenance, and termination of a sustained data exchange require a fair amount of coordination and cooperation among stations. Procedures for the management of this exchange are required.

We shall see in this chapter that a data link protocol that satisfies these requirements is a rather complex affair. We begin by looking at two key mechanisms that are part of data link control: flow control and error control. Following this background we look at the most important example of a data link control protocol: HDLC (high-level data link control). This protocol is important for two reasons: First, it is a widely used standardized data link control protocol. Second, HDLC serves as a baseline from which virtually all other important data link control protocols are derived. Finally, an appendix to this chapter addresses some performance issues relating to data link control.

Flow control is a technique for assuring that a transmitting entity does not overwhelm a receiving entity with data. The receiving entity typically allocates a data buffer of some maximum length for a transfer. When data are received, the receiver must do a certain amount of processing before passing the data to the higher-level software. In the absence of flow control, the receiver's buffer may fill up and overflow while it is processing old data [8]. It has the advantages of showing time dependencies and illustrating the correct send-receive relationship. Each arrow represents a single frame transiting a data link between two stations. The data are sent in a sequence of frames, with each frame containing a portion of the data and some control information.

The time it takes for a station to emit all of the bits of a frame onto the medium is the transmission time; this is proportional to the length of the frame. The propagation time is the time it takes for a bit to traverse the link between source and destination. For this section, we

assume that all frames that are transmitted are successfully received; no frames are lost and none arrive with errors. Furthermore, frames arrive in the same order in which they are sent. However, each transmitted frame suffers an arbitrary and variable amount of delay before reception. On a direct point-to-point link, the amount of delay is fixed rather than variable. However, a data link control protocol can be used over a network connection, such as a circuit-switched or ATM network, in which case the delay may be variable.

The simplest form of flow control, known as stop-and-wait flow control, works as follows. A source entity transmits a frame. After the destination entity receives the frame, it indicates its willingness to accept another frame by sending back an acknowledgment to the frame just received. The source must wait until it receives the acknowledgment before sending the next frame. The destination can thus stop the flow of data simply by withholding acknowledgment. This procedure works fine and, indeed, can hardly be improved upon when a message is sent in a few large frames. However, it is often the case that a source will break up a large block of data \sinto smaller blocks and transmit the data in many frames. This is done for the following reasons:

The longer the transmission, the more likely that there will be an error, necessitating retransmission of the entire frame. With smaller frames, errors are detected sooner, and a smaller amount of data needs to be retransmitted. On a shared medium, such as a LAN, it is usually desirable not to permit one station to occupy the medium for an extended period, thus causing long delays at the other sending stations. The transmission process over time. In both cases, the first four snapshots show the process of transmitting a frame containing data, and the last snapshot shows the return of a small acknowledgment frame. Note that for the line is always underutilized and even for the line is inefficiently utilized. In essence, for very high data rates, for very long distances between sender and receiver, stop-and-wait flow control provides inefficient line utilization.

If we assume the frame transmission time is negligible (very small ACK frame) and that the ACK is sent immediately, the ACK arrives at T at this point, T can begin transmitting a new frame. Now consider a 1-Mbps link between two ground stations that communicate via a satellite relay. A geosynchronous satellite has an altitude of roughly 36,000 km. Then For a frame length of 8000 bits, as a guide, we can work through the same steps as before. In this case, it takes 240 ms for the leading edge of the frame to arrive and an additional 8 ms for the entire frame to arrive. The ACK arrives back at T at The actual transmission time for the first frame was 8 ms, but the total time to transmit the first frame and receive an ACK is 488 ms. Let us examine how this might work for two stations, A and B, connected via a full-duplex link. Station B allocates buffer space for W frames. Thus, B can accept W frames, and A is allowed to send W frames without waiting for any acknowledgments. To keep track of which frames have been acknowledged, each is labelled with a sequence number.

B acknowledges a frame by sending an acknowledgment that includes the sequence number of the next frame expected. This acknowledgment also implicitly announces that B is prepared to receive the next W frames, beginning with the number specified. This scheme can also be used to acknowledge multiple frames. For example, B could receive frames 2, 3, and 4 but withhold acknowledgment until frame 4 has arrived. By then returning an acknowledgment with sequence number 5, B acknowledges frames 2, 3, and 4 at one time. A maintains a list of sequence numbers that it is allowed to send, and B maintains a list of sequence numbers that it is prepared

to receive. Each of these lists can be thought of as a window of frames. The operation is referred to as sliding-window flow control.

Several additional comments need to be made. Because the sequence number to be used occupies a field in the frame, it is limited to a range of values. For example, for a 3-bit field, the sequence number can range from 0 to 7. Accordingly, frames are numbered modulo 8; that is, after sequence number 7, the next number is 0. In general, for a k-bit field the range of sequence numbers is 0 through and frames are numbered modulo As will be shown subsequently, the maximum window size is a useful way of depicting the sliding-window process. The shaded rectangle indicates the frames that may be sent; in this figure, the sender may transmit five frames, beginning with frame 0. Each time a frame is sent, the shaded window shrinks; each time an acknowledgment is received, the shaded window grows. Frames between the vertical bar and the shaded window have been sent but not yet acknowledged. As we shall see, the sender must buffer these frames in case they need to be retransmitted. The window size need not be the maximum possible size for a given sequence number length. For example, using a 3-bit sequence number, a window size of 5 could be configured for the stations using the sliding-window flow control protocol.

The example assumes a 3-bit sequence number field and a maximum window size of seven frames. Initially, A \sand B have windows indicating that A may transmit seven frames, beginning with frame 0 (F0) (F0). After transmitting three frames (F0, F1, F2) without acknowledgment, A has shrunk its window to four frames and maintains a copy of the three transmitted frames. The window indicates that A may transmit four frames, beginning with frame number 3. B then transmits an RR (receive ready) 3, which means. “I have received all frames up through frame number 2 and am ready to receive frame number 3; in fact, I am prepared to receive seven frames, beginning with frame number 3.” With this acknowledgment, A is back up to permission to transmit seven frames, still beginning with frame 3; also A may discard the buffered frames that have now been acknowledged. A proceeds to transmit frames 3, 4, 5, and 6. B returns RR 4, which acknowledges F3, and allows transmission of F4 through the next instance of F2. By the time this RR reaches a, it has already transmitted F4, F5, and F6, and therefore a may only open its window to permit sending four frames beginning with F7.

The mechanism so far described provides a form of flow control: The receiver must only be able to accommodate seven frames beyond the one it has last acknowledged. Most data link control protocols also allow a station to cut off the flow of frames from the other side by sending a Receive Not Ready (RNR) message, which acknowledges former frames but forbids transfer of future frames. Thus, RNR 5 means “I have received all frames up through number 4 but am unable to accept any more at this time.” At some subsequent point, the station must send a normal acknowledgment to reopen the window.

So far, we have discussed transmission in one direction only. If two stations exchange data, each needs to maintain two windows, one for transmit and one for receive, and each side needs to send the data and acknowledgments to the other. To provide efficient support for this requirement, a feature known as piggybacking is typically provided. Each data frame includes a field that holds the sequence number of that frame plus a field that holds the sequence number used for acknowledgment.

Thus, if a station has data to send and an acknowledgment to send, it sends both together in one frame, saving communication capacity. Of course, if a station has an acknowledgment but no

data to send, it sends a separate acknowledgment frame, such as RR or RNR. If a station has data to send but no new acknowledgment to send, it must repeat the last acknowledgment sequence number that it sent. This is because the data frame includes a field for the acknowledgment number, and some value must be put into that field. When a station receives a duplicate acknowledgment, it simply ignores it.

Sliding-window flow control is potentially much more efficient than stop-andwait flow control. The reason is that, with sliding-window flow control, the transmission link is treated as a pipeline that may be filled with frames in transit. In contrast, with stop-and-wait flow control, only one frame may be in the pipe at a time. Appendix 7A quantifies the improvement in efficiency. Error control refers to mechanisms to detect and correct errors that occur in the transmission of frames. As before, data are sent as a sequence of frames; frames arrive in the same order in which they are sent; and each transmitted frame suffers an arbitrary and potentially variable amount of delay before reception. In addition, we admit the possibility of two types of errors:

For the satellite configuration, it takes 488 ms for an ACK to the first frame to \sbe received. It takes 8 ms to transmit one frame, so the sender can transmit 61 frames by the time the ACK to the first frame is received. With a window field of 6 bits or more, the sender can transmit continuously, or a rate of one frame every 8 ms. If the window size is 7, using a 3-bit window field, then the sender can only send \s7 frames and then must wait for an ACK before sending more. In this case, the sender can transmit at a rate of 7 frames per 488 ms, or about one frame every 70 ms. With stop-and-wait, a rate of only one frame per 488 ms is possible.

This number represents the amount of time needed to send a frame. Other figures in this chapter do not depict this period for the sake of simplicity. These forms are all dependent on the use of the flow control strategies. The previously described stop-and-wait flow control method is the foundation of stop-and-wait ARQ. The source station must wait for an acknowledgement after sending one frame (ACK). Until the source station receives the response from the destination station, no more data frames may be transferred. Two different types of mistakes might happen. Secondly, there's a chance that the frame will be damaged when it gets there. The error-detection method mentioned previously is used by the receiver to identify this, and the frame is then simply discarded. The source station has a timer to take this possibility into consideration. The source station waits for an acknowledgement after sending a frame. The identical frame is transmitted again if no acknowledgment is received by the time the timeout ends. It should be noted that this approach necessitates that the transmitter hold onto a duplicate of each broadcast frame until the frame receives an acknowledgement.

A damaged acknowledgement is the second kind of mistake. Think about the following circumstance. Sending a frame is Station A. Station B receives the frame appropriately and sends back an acknowledgement (ACK). The ACK was harmed during transit and is not recognised by A; as a result, A will time out and transmit the identical frame again. When this duplicate frame shows up, B accepts it. As a result, B has accepted two copies of the same frame as distinct. Positive acknowledgments are of the form ACK0 and ACK1, and frames are alternatively tagged with 0 or to get around this issue. An ACK0 acknowledges reception of a frame with the number 1 and signals that the receiver is prepared for a frame with the number 0 in accordance with the sliding-window standard.

The two sorts of faults are shown in the picture. As a result of A's third frame being lost or damaged, B does not respond with an ACK. A times out and sends the frame again. Later, a sends a frame with the number 1 but the ACK0 is misplaced. A sends the same frame again after timing out. B discards the second frame but returns an ACK0 to each when it gets two frames in a row with the same label. Stop-and-wait ARQ's simplicity is its main benefit. Stop-and-wait is an ineffective method, which is its main drawback. It is possible to modify the sliding-window flow control technique often referred to as continuous ARQ to allow for more effective line utilization.

The most popular kind of error control based on sliding-window flow control is known as go-back-N ARQ. This technique allows a station to deliver a string of frames that are progressively numbered modulo a maximum value. Window size is used to calculate the number of unacknowledged frames that are still pending.

B throws away duplicate PDU frames. Technique for sliding-window flow control: 0 ACK 0 Time A B The destination will acknowledge arriving frames as normal (or use piggybacked acknowledgement) if there are no mistakes. The following rules describe how the destination station may issue a negative acknowledgement for a frame if it notices an error in that frame. Up until the frame in mistake is successfully received, the destination station will ignore that frame as well as any subsequent ones that come in. The source station must thus retransmit the incorrect frame together with any consecutive frames that were broadcast in the interval when it gets a REJ.

Assume station A is transmitting frames to station B. A starts an acknowledgement timer for the most recently sent frame after each transmission. Assume that A has just sent frame I and that B had previously successfully received frame. A broken frame. Invalid frames are discarded by B and no further action is taken as a consequence of them if B finds an error in the frame or if it is so damaged that B is not even aware that it has received a frame.

A transmits the frame after an acceptable amount of time has passed. A must resend frames I through n when B gets a frame out of sequence and sends a REJ i.A does not immediately transmit further frames. B doesn't get anything and doesn't give back either an RR or a REJ. After A's timeout ends, it transmits an RR frame with a P bit set to 1, which B sees as a command that has to be acknowledged by sending an RR signaling the next frame that it anticipates, which is frame i. Frame I is retransmitted by A once it gets the RR. As an alternative, A might just send out frame I again when its timer runs out.

It is possible that A will get a later RR to a subsequent frame and that it will arrive before the timer associated with frame I expires since acknowledgments are cumulative (for example, RR 6 signifies that all frames through 5 are acknowledged) broadcasts an RR command as in Example 1b if its timeout expires. The P-bit timer, a different timer, is set. A's P-bit timer will run out if B fails to react to the RR command or if an error occurs while sending its answer. At this point, A will restart the P-bit timer and issue a fresh RR command in an effort to attempt again. Several repetitions of this approach are attempted. A starts a reset operation if, after a certain number of tries, it is unable to get an acknowledgement.

The receiver, on the other hand, must include logic to reorder the frame in question into the correct sequence and must have a buffer big enough to hold post-SREJ frames until the frame in mistake is retransmitted. For the transmitter to be able to send a frame out of order, more

complicated logic is also needed. Select-reject ARQ is substantially less popular than go-back-N ARQ due to these issues. Since there is a significant propagation delay involved, selective reject is a good option for a satellite connection. Compared to goback-N, the window size restriction is more stringent for selective-reject.

A retransmits frame 0 after running out of time. B's receive window has already been advanced to accommodate frames 7, 0, 1, 2, 3, and 5. Inferring that frame 7 has been lost and that this is a new frame 0, which it accepts, is what it does.So until a genuine frame 4 is received, B keeps accepting incoming frames and buffering them. The frames may then be sent to higher-layer software via B in the correct sequence. HDLC is the most significant data link control protocol (ISO 3009, ISO 4335). In addition to being extensively utilised, HDLC also served as the model for several other significant data link control protocols that make use of the same or very similar formats and operating principles. HDLC specifies three station types, two connection configurations, and three data transmission modes of operation to accommodate a range of applications.

When used with an imbalanced setup, the normal response mode (NRM). A secondary may only send data in response to a command from the main, although the primary may begin data transmission to a secondary. Utilize the asynchronous response mode (ARM) when the configuration is imbalanced. The secondary may start a transmission without the primary's express consent. The line's initiation, error recovery, and logical disconnection remain the primary's duty. In multidrop lines, which connect a number of terminals to a host computer, NRM is employed. Each terminal is surveyed by the computer for input. A point-to-point connection connecting a terminal or other peripheral to a computer is a common use for NRM. The most popular of the three modes, ABM uses a full-duplex point-to-point connection more effectively since there is no polling overhead. Seldom utilized, ARM may be useful in certain unique circumstances where a secondary may need to commence transmission.

CONCLUSION

Data Link Control (DLC) protocols are a set of standards and procedures used for reliable and efficient data transfer between two devices over a communication network [9]–[11]. These protocols are implemented at the Data Link layer of the OSI model and provide a range of functions such as error detection and correction, flow control, and data synchronization. DLC protocols are critical in establishing and maintaining logical connections between devices, ensuring that data is delivered accurately and securely. They help prevent data collisions and enable the effective transmission of data across a network

REFERENCES

[1] S. Maurya, V. Kumar Nayak, and D. A Nagaraju, “Implementation of Data Link Control Protocols in Wired Network,” *Int. J. Eng. Trends Technol.*, 2014, doi: 10.14445/22315381/ijett-v18p211.

[2] K. S. Chan, S. Chan, and K. T. Ko, “A data link control protocol for broadband wireless networks with adaptive coding rate,” *Int. J. Commun. Syst.*, 2006, doi: 10.1002/dac.769.

[3] G. A. Aderounmu, E. R. Adagunodo, and A. D. Akinde, “Performance comparison of data-link control protocol for wireless asynchronous transfer mode network,” *Int. J. Comput. Appl.*, 2002, doi: 10.1080/1206212X.2002.11441674.

[4] R. J. Sanchez, F. F. Wahhab, J. B. Evans, V. S. Frost, and G. J. Minden, "Design and evaluation of an adaptive data link control protocol for wireless ATM networks," *Conf. Rec. / IEEE Glob. Telecommun. Conf.*, 1998, doi: 10.1109/glocom.1998.775931.

[5] K. S. Chan, S. Chan, and K. T. Ko, "Data link control protocol for wireless ATM networks with adaptive coding rate," *IEEE ATM Work. Proc.*, 2000.

[6] H. Semira, M. Benouaret, and S. Harize, "Implementation of a Single-Channel HDLC Controller on FPGA," *Int. J. Comput. Appl.*, 2015, doi: 10.5120/ijca2015907208.

[7] T. Guha, I. Pal, R. Basak, F. Khan, and S. A. Khan, "Design and Implementation of HDLC Protocol using VHDL technique," in *2020 4th International Conference on Electronics, Materials Engineering and Nano-Technology, IEMENTech 2020*, 2020. doi: 10.1109/IEMENTech51367.2020.9270075.

[8] J. Tellechea-Luzardo *et al.*, "Versioning biological cells for trustworthy cell engineering," *Nat. Commun.*, 2022, doi: 10.1038/s41467-022-28350-4.

[9] J. Kumar, A. Singh, and H. S. Bhadauria, "Link discontinuity and optimal route data delivery for random waypoint model," *J. Ambient Intell. Humaniz. Comput.*, 2021, doi: 10.1007/s12652-021-03032-z.

[10] A. Larmo, A. Ratilainen, and J. Saarinen, "Impact of coAP and MQTT on NB-IoT system performance," *Sensors (Switzerland)*, 2019, doi: 10.3390/s19010007.

[11] J. Ali, G. M. Lee, B. H. Roh, D. K. Ryu, and G. Park, "Software-defined networking approaches for link failure recovery: A survey," *Sustain.*, 2020, doi: 10.3390/su12104255.

CHAPTER 20

MULTIPLEXING TECHNIQUES FOR EFFICIENT DATA TRANSMISSION: A COMPREHENSIVE REVIEW

Pankaj Kumar Goswami, Associate Professor
Department of Electronics and Communication Engineering,
Teerthanker Mahaveer University, Moradabad, Uttar Pradesh, India
Email Id- g.pankaj1@gmail.com

ABSTRACT:

Multiplexing is a technique used to transmit multiple data streams over a single communication channel, thereby increasing the efficiency of data transmission. There are several types of multiplexing techniques, including time-division multiplexing (TDM), frequency-division multiplexing (FDM), and wavelength-division multiplexing (WDM), among others. In TDM, each data stream is given a time slot in a fixed cycle, allowing multiple data streams to be transmitted over a single channel. In FDM, different data streams are assigned different frequency bands within a channel, allowing them to be transmitted simultaneously. WDM is a technique used in fiber-optic communication systems, where different wavelengths of light are used to transmit different data streams over the same fiber.

KEYWORDS:

Communication System, Data Stream, Data Transmission, Fiber Optics, Wave Length.

INTRODUCTION

A kind of multiplexing is utilised to effectively use high-speed telecommunications connections. A higher transmission capacity may be shared by various transmission sources thanks to multiplexing. The two similar the use of frequency division multiplexing with analogue communications is possible. By giving each signal a unique frequency band, many signals may be conveyed concurrently on the same medium. Each signal must be moved to the necessary frequency range using modulation equipment, and the modulated signals must be combined using multiplexing equipment.

Analog signals conveying digital data as well as digital signals themselves may employ synchronous time division multiplexing. Data from several sources are conveyed in repeating frames in this kind of multiplexing. Each source is given one or more time slots every frame, which each consist of a collection of time slots. The result is the interleaving of data fragments from several sources [1]–[3]. When it comes to supporting terminals, statistical time division multiplexing is often more effective than synchronous TDM. Time slots are not already allotted to certain data sources while using statistical TDM. Instead, user data is delayed and sent as quickly as feasible within open time intervals.

We discussed effective methods for using a data connection under a lot of demand. It is often preferable to have many frames outstanding when two devices are linked via a point-to-point connection so that the data channel does not get congested between the stations. Now think about

the reverse issue. Two communicating stations won't usually use up all of a data link's capacity. It should be feasible to share that potential for effectiveness. Multiplexing is a general name for this kind of sharing. The connection has the capacity to transport n different data channels. Data from the n input lines are combined (multiplexed) by the multiplexer before being sent across a higher-capacity data connection. The DE multiplexer receives the stream of multiplexed data, divides it (DE multiplexes) into channels, and sends the channels' data to the appropriate output lines [4].

In other words, for a given application and over a given distance, the cost per kbps decreases as the transmission facility's data rate increases. Similar to this, as data rate increases, transmission and reception equipment costs per kbps decrease. The majority of personal data communication devices only need moderate data rate support. For instance, a data rate of between 9600 bps and 64 kbps is often sufficient for many terminal and personal computer applications that do not include Web access or complex graphics. The sentences above used the terminology of data communicating devices. The same is true for voice conversations. That is, the cost per speech channel decreases as a transmission facility's voice channel capacity increases, and just a small amount of capacity is needed for a single voice channel.

The three different multiplexing strategies are the main focus of this chapter. Anybody who has ever used a radio or television set is likely aware with the first, called frequency division multiplexing (FDM), which is also the most widely used. The second is synchronous TDM, a specific kind of time division multiplexing (TDM). For multiplexing digital audio streams and data streams, this is often utilized. The third form makes the multiplexer more sophisticated in an effort to increase synchronous TDM's efficiency. Statistical TDM, asynchronous TDM, and intelligent TDM are some of the names it goes by. The term statistical TDM is used in this work to emphasize one of its key characteristics. The digital subscriber line, which combines synchronous TDM and FDM technology, is the subject of our last examination [5], [6].

When the practical bandwidth of the transmission media is greater than the necessary bandwidth of the signals to be sent, FDM is feasible. If each signal is modulated onto a distinct carrier frequency and the carrier frequencies are spaced apart enough such that the bandwidths of the signals do not considerably overlap, several signals may be conveyed concurrently. A multiplexer receives sources and modulates each signal onto a separate frequency. Each modulated signal needs a certain channel, or bandwidth, centered on its carrier frequency. Guard bands, which are unused areas of the spectrum, are utilized to divide the channels in order to avoid interference.

Analog signaling is used to transfer the composite signal via the medium. However keep in mind that the input signals might be digital or analogue. When using digital input, modems must be used to convert the digital signals to analogue. In either scenario, modulation is required to shift each analogue input signal to the proper frequency range. The same transmission medium must multiplex a number of analogue or digital signals. Each signal is modulated onto a carrier, which is referred to as a subcarrier since numerous carriers are to be employed. Modulation of any kind may be used. A composite baseband1 signal is created by adding the resultant analog, modulated signals. The signal's spectrum is altered to be in the middle of the bandwidths of the different signals must not considerably overlap for this technique to function. The original signals cannot be recovered in any other case.

On a carrier signal, a black-and-white video signal is AM modulated. We would anticipate the modulated signal to have a bandwidth of 8 MHz centered on the 4 MHz of the baseband video stream. The signal is sent via a sideband filter to largely reduce the lower sideband in order to save bandwidth. The resultant signal has a range of around to Color information is sent via a separate color carrier. There is almost no interference because of the distance between these two.

Lastly, the audio component of the signal is modulated outside of its own effective bandwidth. The audio signal is given a 50 kHz bandwidth. The video, colour, and audio signal carriers are located at 1.25 MHz, 4.799545 MHz, and 5.75 MHz above the bottom border of the band, respectively, such that the composite signal may fit within a 6-MHz bandwidth. As a result, numerous TV signals, each having a bandwidth of 6 MHz, may be frequency division multiplexed over a CATV cable. The overall bandwidth B of the FDM signal s(t) is where. A appropriate media may be used to convey this analogue signal. The FDM signal is demodulated at the receiving end before being routed through n band pass filters, each of which is focused on and has a bandwidth for The signal is once again divided into its constituent pieces in this manner. The original signal is then recovered by demodulating each component.

Crosstalk is the first possibility and happens when the spectra of nearby component signals greatly overlap. A 4-kHz bandwidth is sufficient for speech transmissions since their effective bandwidth is only 3100 Hz (300–3400). This bandwidth also accommodates the signal spectra generated by modems for voiceband transmission between 60 and 68 kHz, with an interval of 8 kHz. We decide to solely send the lowest sideband in order to effectively utilise the available bandwidth. The spectrum shows what is produced when three voice signals are utilised to modulate carriers at 64, 68, and 72 kHz and only the lowest sideband of each is captured. Voiceband signals may be sent across high-capacity transmission lines, such coaxial cable and microwave systems, using the long-distance carrier system offered in the United States and around the globe.

DISCUSSION

FDM is the first and most widely used method for using high-capacity lines. In order to handle transmission systems of varied capacities, AT&T has established a hierarchy of FDM schemes in the United States. Under the direction of ITU-T, a comparable, but regrettably not identical, system has been implemented globally. The 60-channel supergroup is the next fundamental building component, and it is created by frequency division multiplexing five group signals. At this stage, a subcarrier is used to modulate each group and it is considered as a single signal with a 48 kHz bandwidth. The subcarriers range in frequency from 420 to 612 kHz in 48 kHz steps. The final signal ranges from 312 to 552 kHz.

Keep in mind that the original speech or data stream may undergo many modulations. For instance, an analogue speech signal might be created by QPSK encoding a digital stream. A 76-kHz carrier might then be modulated using this signal to create a part of a group signal. A 516-kHz carrier might then be modulated using this group signal to create a part of a supergroup signal. The original data may be distorted at each step; for instance, if the modulator/multiplexer contributes noise or has nonlinearities.The term dense wavelength division multiplexing (DWDM) is often used in the literature. There isn't a formal or accepted meaning for this phrase. The phrase implies the usage of additional channels, spaced closer together than in regular WDM. Channel spacing of 200 GHz or less is often regarded as dense [7], [8].

When the attainable data rate (sometimes, regrettably, referred to as bandwidth) of the media exceeds the data rate of the digital signals to be sent, synchronous time division multiplexing is feasible. By interleaving sections of each signal in time, several digital signals (or analogue signals containing digital data) may be sent over a single transmission line. Table 8.2 ITU WDM Channel Spacing, or at the bit level, may be used for the interleaving (G.692)

The same transmission medium is to be multiplexed with a variety of signals. The signals are often digital signals that convey digital data. Each source's incoming data is momentarily buffered. Typically, a buffer has a length of one bit or one character. In order to create a composite digital data stream, the buffers are scanned one at a time. Each buffer is completely emptied during the scan procedure before further data may be added. Hence, the data rate of must at least match the total of the data rates of it is possible to send the digital signal using the mi1t2 protocol. The information is arranged into frames. A cycle of time slots is included in each frame. Each data source has one or more slots in each frame set aside for it. A channel is the collection of slots that are reserved for one source from frame to frame. The transmitter buffer length, which is commonly a bit or a byte, matches the slot length (character).

Both synchronous and asynchronous sources may employ the byte-interleaving approach. One character of data is included in each time period. Generally, each character's start and stop bits are removed before transmission and then reinserted by the receiver to increase efficiency. The bit-interleaving approach may be used to both synchronous and asynchronous sources. There is just one bit in each time slot. The interleaved data are demultiplexed and sent to the right destination buffer at the receiver. There is an identical output destination that will receive the output data at the same pace as it was created for each input source.

Since the time slots are set and preassigned to sources, synchronous TDM is not named synchronous because synchronous transmission is employed. Regardless of whether a source has data to communicate, the time slots for each source are sent. Of course, FDM also operates in this manner. Both times, unnecessary resources are used to achieve implementation simplicity. Nonetheless, even when fixed assignment is utilised, synchronous TDM devices can handle sources with various data rates. As an example, the fastest input device may be given numerous slots every cycle while the slowest one slot per cycle. The reader will notice that the headers and trailers that we have come to recognise with synchronous transmission are absent from the transmitted data stream. The rationale is because a data connection protocol's control mechanisms are not required. This aspect merits reflection, which we accomplish by focusing on two important data connection control mechanisms: flow control and error control. It should be obvious that flow control is not required for the multiplexer and demultiplexer. The multiplexer and demultiplexer are built to function at the fixed data rate on the multiplexed line. Imagine, however, that one of the several output lines connects to a machine that is momentarily unable to take data. Should TDM frame transmissions stop? Evidently not, given that the remaining output lines anticipate receiving data at certain intervals. The issue may be resolved by having the saturated output device stop the data from the matching input device from flowing. As a result, the channel in question will temporarily carry empty slots, but the overall transmission rate of the frames will remain the same.

The justification for error prevention is the same. Requiring the retransmission of an entire TDM frame because of a single channel mistake is unacceptable. The devices utilising the other channels are not asking for a retransmission, nor would they be aware that another device on

another channel has requested one. A data link control protocol, such as HDLC, may be used to offer flow control and error control on a per-channel basis provides a condensed illustration. We presume two HDLC-enabled data sources. One is sending a stream of HDLC frames, each carrying three octets of data, while the other is sending HDLC frames, each carrying four. While bit interleaving is more common, for the sake of clarity, we assume that character-interleaved multiplexing is used.

Take note of what is occurring. For transmission across the multiplexed line, the octets of the HDLC frames from the two sources are mixed together. The fact that the HDLC frames have in some ways lost their integrity may make the reader immediately uneasy with this graphic. Each frame check sequence (FCS) on the line, for instance, applies to a random assortment of bits. Even the FCS is not completely intact. Before they are detected by the device on the other end of the HDLC connection, the fragments are, however, appropriately reassembled. In this way, the multiplexing/demultiplexing process is invisible to the associated stations, giving the impression that each communicating pair of stations is on a separate connection.

Framing we have shown that the whole TDM link can be managed without a link control protocol. But, there is a fundamental prerequisite for framing. The lack of flag or SYNC characters to bracket TDM frames necessitates the employment of some other method to ensure frame synchronisation. Framing synchronisation must be kept up because if the source and destination are out of sync, data on all channels will be lost.It is improbable that this pattern will persist on a data channel. Hence, a receiver compares the arriving bits of one frame location to the anticipated pattern in order to synchronise. In the event that the pattern is not a match, further bit locations are looked for until the pattern is sustained throughout many frames. The receiver keeps an eye on the framing bit channel once frame synchronisation has been achieved. In the event that the pattern fails, the receiver must once again switch to framing search mode. Heart stuffing the synchronisation of the various data sources is arguably the trickiest issue in the design of a synchronous time division multiplexer. If each source has its own clock, any difference between clocks could result in synchronisation loss. Additionally, the input data streams' data rates aren't always related by a straightforward rational number.

An effective solution to both of these issues is the pulse stuffing technique. When pulse stuffing is used, the multiplexer's outgoing data rate excluding framing bits exceeds the sum of its maximum instantaneous incoming rates. By packing extra dummy bits or pulses into each incoming signal until its frequency matches that of a locally generated clock signal, the extra capacity is utilised. In order to be recognised and eliminated at the demultiplexer, the stuffed pulses are inserted at predetermined locations in the multiplexer frame format. A kind of multiplexing is utilised to effectively use high-speed telecommunications connections. A higher transmission capacity may be shared by various transmission sources thanks to multiplexing. The two similar Frequency division multiplexing (FDM) and temporal division multiplexing are examples of multiplexing (TDM).

The use of frequency division multiplexing with analogue communications is possible. By giving each signal a unique frequency band, many signals may be conveyed concurrently on the same medium. Each signal must be moved to the necessary frequency range using modulation equipment, and the modulated signals must be combined using multiplexing equipment. Analog signals conveying digital data as well as digital signals themselves may employ synchronous time division multiplexing. Data from several sources are conveyed in repeating frames in this

kind of multiplexing. Each source is given one or more time slots every frame, which each consist of a collection of time slots. The result is the interleaving of data fragments from several sources.

When it comes to supporting terminals, statistical time division multiplexing is often more effective than synchronous TDM. Time slots are not already allotted to certain data sources while using statistical TDM. Instead, user data is delayed and sent as quickly as feasible within open time intervals.

We discussed effective methods for using a data connection under a lot of demand in Chapter 7. It is often preferable to have many frames outstanding when two devices are linked via a point-to-point connection so that the data channel does not get congested between the stations. Now think about the reverse issue. Two communicating stations won't usually use up all of a data link's capacity. It should be feasible to share that potential for effectiveness. Multiplexing is a general name for this kind of sharing. In other words, for a given application and over a given distance, the cost per kbps decreases as the transmission facility's data rate increases. Similar to this, as data rate increases, transmission and reception equipment costs per kbps decrease. The majority of personal data communication devices only need moderate data rate support. For instance, a data rate of between 9600 bps and 64 kbps is often sufficient for many terminal and personal computer applications that do not include Web access or complex graphics.

The sentences above used the terminology of data communicating devices. The same is true for voice conversations. That is, the cost per speech channel decreases as a transmission facility's voice channel capacity increases, and just a small amount of capacity is needed for a single voice channel. The three different multiplexing strategies are the main focus of this chapter. Anybody who has ever used a radio or television set is likely aware with the first, called frequency division multiplexing (FDM), which is also the most widely used. The second is synchronous TDM, a specific kind of time division multiplexing (TDM). For multiplexing digital audio streams and data streams, this is often utilised. The third form makes the multiplexer more sophisticated in an effort to increase synchronous TDM's efficiency. Statistical TDM, asynchronous TDM, and intelligent TDM are some of the names it goes by. The term statistical TDM is used in this work to emphasise one of its key characteristics. The digital subscriber line, which combines synchronous TDM and FDM technology, is the subject of our last examination.

The same transmission medium must multiplex a number of analogue or digital signals. Each signal is modulated onto a carrier, which is referred to as a subcarrier since numerous carriers are to be employed. Modulation of any kind may be used. A composite baseband1 signal is created by adding the resultant analog,modulated signals. The signal's spectrum is altered to be in the middle of the bandwidths of the different signals must not considerably overlap for this technique to function. The original signals cannot be recovered in any other case. On a carrier signal, a black-and-white video signal is AM modulated. We would anticipate the modulated signal to have a bandwidth of 8 MHz centred on the 4 MHz of the baseband video stream. The signal is sent via a sideband filter to largely reduce the lower sideband in order to save bandwidth. The resultant signal has a range of around to Color information is sent via a separate colour carrier. There is almost no interference because of the distance between these two.

Keep in mind that the original speech or data stream may undergo many modulations. For instance, an analogue speech signal might be created by QPSK encoding a digital stream. A 76-kHz carrier might then be modulated using this signal to create a part of a group signal. A 516-

kHz carrier might then be modulated using this group signal to create a part of a supergroup signal. The original data may be distorted at each step; for instance, if the modulator/multiplexer contributes noise or has nonlinearities.

When the attainable data rate sometimes, regrettably, referred to as bandwidth of the media exceeds the data rate of the digital signals to be sent, synchronous time division multiplexing is feasible. By interleaving sections of each signal in time, several digital signals or analogue signals containing digital data may be sent over a single transmission line. The same transmission medium is to be multiplexed with a variety of signals. The signals are often digital signals that convey digital data. Each source's incoming data is momentarily buffered. Typically, a buffer has a length of one bit or one character. In order to create a composite digital data stream, the buffers are scanned one at a time. Each buffer is completely emptied during the scan procedure before further data may be added. Hence, the data rate of must at least match the total of the data rates of it is possible to send the digital signal using the mi1t2 protocol.

The information is arranged into frames. A cycle of time slots is included in each frame. Each data source has one or more slots in each frame set aside for it. A channel is the collection of slots that are reserved for one source from frame to frame. The transmitter buffer length, which is commonly a bit or a byte, matches the slot length (character). Both synchronous and asynchronous sources may employ the byte-interleaving approach. One character of data is included in each time period. Generally, each character's start and stop bits are removed before transmission and then reinserted by the receiver to increase efficiency. The bit-interleaving approach may be used to both synchronous and asynchronous sources. There is just one bit in each time slot.

The interleaved data are DE multiplexed and sent to the right destination buffer at the receiver. There is an identical output destination that will receive the output data at the same pace as it was created for each input source. Since the time slots are set and preassigned to sources, synchronous TDM is not named synchronous because synchronous transmission is employed. Regardless of whether a source has data to communicate, the time slots for each source are sent. Of course, FDM also operates in this manner. Both times, unnecessary resources are used to achieve implementation simplicity. Nonetheless, even when fixed assignment is utilised, synchronous TDM devices can handle sources with various data rates. As an example, the fastest input device may be given numerous slots every cycle while the slowest one slot per cycle. The reader will notice that the headers and trailers that we have come to recognise with synchronous transmission are absent from the transmitted data stream. The rationale is because a data connection protocol's control mechanisms are not required. This aspect merits reflection, which we accomplish by focusing on two important data connection control mechanisms: flow control and error control. It should be obvious that flow control is not required for the multiplexer and demultiplexer [9], [10].

The multiplexer and demultiplexer are built to function at the fixed data rate on the multiplexed line. Imagine, however, that one of the several output lines connects to a machine that is momentarily unable to take data. Should TDM frame transmissions stop? Evidently not, given that the remaining output lines anticipate receiving data at certain intervals. The issue may be resolved by having the saturated output device stop the data from the matching input device from flowing. As a result, the channel in question will temporarily carry empty slots, but the overall transmission rate of the frames will remain the same. The justification for error prevention is the

same. Requiring the retransmission of an entire TDM frame because of a single channel mistake is unacceptable. The devices utilising the other channels are not asking for a retransmission, nor would they be aware that another device on another channel has requested one.

CONCLUSION

Multiplexing is the process of combining multiple data streams into a single channel for transmission or communication over a network. It is a crucial technique used in telecommunications and computer networking to efficiently utilize the available bandwidth and increase the overall capacity of the network [11] . Multiplexing is widely used in various applications, such as telephony, cable TV, and internet communications, and it has greatly contributed to the development and growth of modern communication systems. With the increasing demand for high-speed data transmission and the emergence of new technologies such as 5G and the Internet of Things (IoT), multiplexing will continue to play a vital role in shaping the future of communication networks.

REFERENCES

[1] A. S. Whale, J. F. Huggett, and S. Tzonev, “Fundamentals of multiplexing with digital PCR,” *Biomolecular Detection and Quantification*. 2016. doi: 10.1016/j.bdq.2016.05.002.

[2] E. Meyer-Scott, C. Silberhorn, and A. Migdall, “Single-photon sources: Approaching the ideal through multiplexing,” *Rev. Sci. Instrum.*, 2020, doi: 10.1063/5.0003320.

[3] S. Chen, W. Liu, Z. Li, H. Cheng, and J. Tian, “Metasurface-Empowered Optical Multiplexing and Multifunction,” *Advanced Materials*. 2020. doi: 10.1002/ adma. 201805912.

[4] M. S. Frei, M. Tarnawski, M. J. Roberti, B. Koch, J. Hiblot, and K. Johnsson, “Engineered HaloTag variants for fluorescence lifetime multiplexing,” *Nat. Methods*, 2022, doi: 10.1038/s41592-021-01341-x.

[5] M. Yousefi and X. Yangzhang, “Linear and Nonlinear Frequency-Division Multiplexing,” *IEEE Trans. Inf. Theory*, 2020, doi: 10.1109/TIT.2019.2941479.

[6] K. Wang *et al.*, “Simple oligonucleotide-based multiplexing of single-cell chromatin accessibility,” *Mol. Cell*, 2021, doi: 10.1016/j.molcel.2021.09.026.

[7] V. Mylka *et al.*, “Comparative analysis of antibody- and lipid-based multiplexing methods for single-cell RNA-seq,” *Genome Biol.*, 2022, doi: 10.1186/s13059-022-02628-8.

[8] J. Oh *et al.*, “Adjoint-optimized metasurfaces for compact mode-division multiplexing,” *ACS Photonics*, 2022, doi: 10.1021/acsphotonics.1c01744.

[9] B. J. Puttnam, G. Rademacher, and R. S. Luís, “Space-division multiplexing for optical fiber communications,” *Optica*, 2021, doi: 10.1364/optica.427631.

[10] C. Guo *et al.*, “CellTag Indexing: Genetic barcode-based sample multiplexing for single-cell genomics,” *Genome Biol.*, 2019, doi: 10.1186/s13059-019-1699-y.

[11] G. Lin, M. A. B. Baker, M. Hong, and D. Jin, “The Quest for Optical Multiplexing in Bio-discoveries,” *Chem*. 2018. doi: 10.1016/j.chempr.2018.01.009.

CHAPTER 21

SPREAD SPECTRUM: A COMPREHENSIVE STUDY ON THEORY, TECHNIQUES, AND APPLICATIONS FOR SECURE AND EFFICIENT DATA COMMUNICATION

Rahul Sharma, Assistant Professor
Department of Electronics and Communication Engineering,
Teerthanker Mahaveer University, Moradabad, Uttar Pradesh, India
Email Id- drrahuls.iitk@gmail.com

ABSTRACT:

Spread spectrum is a technique used in telecommunications and wireless communication systems to improve the reliability, security, and capacity of the network. This technique spreads the signal over a wider frequency band than is necessary for transmission, making it more resistant to interference and eavesdropping. Spread spectrum has several variants, including direct sequence spread spectrum (DSSS) and frequency hopping spread spectrum (FHSS), among others. DSSS uses a high data rate and a pseudo-random sequence to spread the signal over a wide frequency band, while FHSS rapidly hops between different frequency channels to avoid interference and improve security.

KEYWORDS:

Direct Sequence, Spread Spectrum, Telecommunication, Network, Security.

INTRODUCTION

Input into a channel encoder that produces an analogue signal with a relatively narrow bandwidth around some center frequency. This signal is further modulated using a sequence of digits known as a spreading code or spreading sequence. Typically, but not always, the spreading code is generated by a pseudo noise, or pseudorandom number, generator. The effect of this modulation is to increase significantly the bandwidth (spread the spectrum) of the signal to be transmitted. On the receiving \send, the same digit sequence is used to demodulate the spread spectrum signal [1], [2].

The earliest applications of spread spectrum were military, where it was used for its immunity to jamming. It can also be used for hiding and encrypting signals. Only a recipient who knows the spreading code can recover the encoded information. Several users can independently use the same higher bandwidth with very little interference. This property is used in cellular telephony applications, with a technique known as code division multiplexing (CDM) or code division multiple access (CDMA) (CDMA).

A comment about pseudorandom numbers is in order. These numbers are generated by an algorithm using some initial value called the seed. The algorithm is deterministic and therefore produces sequences of numbers that are not statistically random. However, if the algorithm is good, the resulting sequences will pass many reasonable tests of randomness. Such numbers are often referred to as pseudorandom numbers. The important point is that unless you know the algorithm and the seed, it is impractical to predict the sequence. Hence, only a receiver that shares this information with a transmitter will be able to decode the signal successfully. With

frequency-hopping spread spectrum (FHSS), the signal is broadcast over a seemingly random series of radio frequencies, hopping from frequency to frequency at fixed intervals. A receiver, hopping between frequencies in synchronization with the transmitter, picks up the message. Would-be eavesdroppers hear only unintelligible blips. Attempts to jam the signal on one frequency succeed only at knocking out a few bits of it [3]–[5].

Typically, there are carrier frequencies forming channels. The spacing between carrier frequencies and hence the width of each channel usually corresponds to the bandwidth of the input signal. The transmitter operates in one channel at a time for a fixed interval; for example, the IEEE 802.11 standard uses 300-ms interval. During that interval, some number of bits (possibly a fraction of a bit, as discussed subsequently) is transmitted using some encoding scheme. A spreading code dictates the sequence of channels used. Both transmitter and receiver use the same code to tune into a sequence of channels in synchronization.

A typical block diagram for a frequency-hopping system. For transmission, binary data are fed into a modulator using some digital-toanalog encoding scheme, such as frequency shift keying (FSK) or binary phase shift keying (BPSK) (BPSK). The resulting signal is centered on some base frequency. A pseudonoise (PN), or pseudorandom number, source serves as an index into a table of frequencies; this is the spreading code referred to previously. Each k bits of the PN source specifies one of the carrier frequencies. At each successive interval (each k PN bits), a new carrier frequency is selected. This frequency is then modulated by the signal produced from the initial modulator to produce a new signal with the same shape but now centred on the selected carrier frequency [6]. On reception,

The frequency synthesiser generates a constant-frequency tone whose frequency hops among a set of frequencies, with the hopping pattern determined by k bits from the PN sequence. For simplicity, assume the duration of one hop is the same as the duration of one bit and we ignore phase differences between the data signal and the spreading signal, also called a chipping signal, c(t) (t). Then the product signal during the ith hop during the ith bit is where the frequency of the signal is generated by the frequency synthesiser during the ith hop. Some authors use a somewhat different definition (e.g., [PICK82]) of multiple hops per bit for fast frequency hop, multiple bits per hop for slow frequency hop, and one hop per bit if neither fast nor slow. The more common definition, which we use, relates hops to signal elements rather than bits.

For FHSS, the MFSK signal is translated to a new frequency every seconds by modulating the MFSK signal with the FHSS carrier signal. The effect is to translate the MFSK signal into the appropriate FHSS channel. For a data rate of R, the duration of a bit is seconds and the duration of a signal element is seconds. If is greater than or equal to , the spreading modulation is referred to as slow-frequency-hop spread spectrum; otherwise it is known as fast-frequency-hop spread spectrum [7].

Here we have which means that four different frequencies are used to encode the data input 2 bits at a time. Each signal element is a discrete frequency tone, and the total MFSK bandwidth is we use an FHSS scheme with that is, there are different channels, each of width the total FHSS bandwidth is Each 2 bits of the PN sequence is used to select one of the four channels. That channel is held for a duration of two signal elements, or four bits 1Tc = 2Ts = 4T2. One benefit of this is that a large value of k results in a system that is quite resistant to jamming. For example, suppose we have an MFSK transmitter with bandwidth and a noise jammer of the same

bandwidth and fixed power on the signal carrier frequency. Then we have a ratio of signal energy per bit to noise power density per Hertz of

If frequency hopping is used, the jammer must jam all frequencies. With a fixed power, this reduces the jamming power in any one frequency band to the gain in signal-to-noise ratio, or processing gain. With direct sequence spread spectrum (DSSS), each bit in the original signal is represented by multiple bits in the transmitted signal, using a spreading code. The spreading code spreads the signal across a wider frequency band in direct proportion to the number of bits used. Therefore, a 10-bit spreading code spreads the signal across a frequency band that is 10 times greater than a 1-bit spreading code.

One technique with direct sequence spread spectrum is to combine the digital \information stream with the spreading code bit stream using an exclusive-OR (XOR) (XOR). The XOR obeys the following rules: Note that an information bit of one inverts the spreading code bits in the combination, while an information bit of zero causes the spreading code bits to be transmitted without inversion. The combination bit stream has the data rate of the original spreading code sequence, so it has a wider bandwidth than the information stream. In this example, the spreading code bit stream is clocked at four times the information rate.

The spectrum spreading achieved by the direct sequence technique is easily determined. In our example, the information signal has a bit width of T, which is equivalent to a data rate of 1/T. In that case, the spectrum of the signal, depending on the encoding technique, is roughly 2/T. Similarly, the spectrum of the PN signal shows the resulting spectrum spreading. The amount of spreading that is achieved is a direct result of the data rate of the PN stream. CDMA is a multiplexing technique used with spread spectrum. The scheme works in the following manner. We start with a data signal with rate D, which we call the bit data rate. We break each bit into k chips according to a fixed pattern that is specific to each user, called the user's code. The new channel has a chip data rate of kD chips per second[8]. As an illustration we consider a simple example5 with It is simplest to characterise a code as a sequence of 1s and the codes for three users, A, B, and C, each of which is communicating with the same base station receiver, R.

DISCUSSION

The subscript u on S simply indicates that u is the user that we are interested in. Let's suppose the user u is actually A and see what happens. If A sends a 1 bit, then d is and the preceding computation using becomes please note that it is always the case that no matter what sequence of and 1s that d is, and that the only d's resulting in the extreme values of 6 and are A's code and its complement, respectively. So if produces a we say that we have received a 1 bit from A; if produces a we say that we have received a 0 bit from user A; otherwise, we assume that someone else is sending information or there is an error. So why go through all this? The reason becomes clear if we see what happens if user B is sending and we try to receive it with that is, we are decoding with the wrong code, A's. If B sends a 1 bit, then

Thus, the unwanted signal (from B) does not show up at all. You can easily verify that if B had sent a 0 bit, the decoder would produce a value of 0 for again. This means that if the decoder is linear and if A and B transmit signals and, respectively, at the same time, then since the decoder ignores B when it is using A's code. The codes of A and B that have the property that are called orthogonal. Such codes are very nice to have but there are not all that many of them. More common is the case when is small in absolute value when Then it is easy to distinguish between

the two cases when and when In our example but In the latter case the C signal would make a small contribution to the decoded signal instead of 0. Using the decoder, the receiver can sort out transmission from u even when there may be other users broadcasting in the same cell. In practice, the CDMA receiver can filter out the contribution from unwanted users or they appear as low-level noise. However, if there are many users competing for the channel with the user the receiver is trying to listen to, or if the signal power of one or more competing signals is too high, perhaps because it is very near the receiver (the "near/far" problem), the system breaks down.

Let us now look at CDMA from the viewpoint of a DSSS system using BPSK. For each user, the data stream to be transmitted, is BPSK modulated to produce a signal with a bandwidth of and then multiplied by the spreading code for that user, All of the signals, plus noise, are received at the receiver's antenna. Suppose that the receiver is attempting to recover the data of user 1. The incoming signal is multiplied by the spreading code of user 1 and then demodulated. The effect of this is to narrow the bandwidth of that portion of the incoming signal corresponding to user 1 to the original bandwidth of the unspread signal, which is proportional to the data rate. Incoming signals from W ci1t2. s di1t2, (a) User's codes

In cases when the channel is in a deep fade, diversity tactics are used. The likelihood that all signal components will fade concurrently increases if several copies of the same information signal are sent over separate fading channels lowered a great deal. We may send the receiver L independent fading copies of the same information signal in a variety of ways. While using frequency diversity, L carriers are used to carry the information signal. The distance between the following carriers is equal to or greater than the channel's coherent bandwidth. In order to attain large data rates and low bit error rates in frequency selective channels, orthogonal frequency division multiplexing (OFDM) transmission is a well-known technology. Several antennas are a frequent technique for producing variety. The same information signal is broadcast by many transmitting antennas, and it is received by numerous receiving antennas through uncorrelated fading routes as independently fading copies of the original signal. Provides a comparison of spatial diversity approaches used in mobile radio. The well-known Multiple-Input Multiple-Output (MIMO) system takes use of antenna diversity to reduce bit error rates and increase channel capacity in fading settings. Another diversity technique is temporal diversity, which involves delivering the same information signal in L separate time slots to create a L independent fading version of the signal.

The gap between the next time slots is equal to or greater than the channel's coherence time. By interleaving the transmitted signals and employing channel codes, time diversity is used in current communication systems. With this approach, the data symbol may be sent more than once using a different symbol period and arrive to the antennas of the receiver through several spatial pathways. Another example of a multidiversity system is the MIMO-OFDM system, which uses temporal, frequency, and spatial diversities to improve the efficiency of data transmission via wireless fading channels. The symbols in the MIMO-OFDM system are encoded using block codes for space-time-frequency (STF). The encoded symbol is sent many multiple once utilising various transmitting antennas, carrier frequencies, and time intervals. The diversity gain at the receiver is achieved by the uncorrelated fading gains resulting from the uncorrelated spatial pathways, the various transmitting time slots, and the various transmitting carriers. Compared to space-time coded MIMO systems, this system performs better and has a substantial diversity gain [9] .

Several antennas are required at both the transmitter and the receiver in systems that exploit spatial diversity, such as MIMO systems. The construction of the transmitter and receiver is complicated because many antennas need several RF drivers (power amplifiers at the transmitter and low noise amplifiers at the receiving). In order to have uncorrelated fading routes and to lessen cross-correlation and interference between the antennas, there should be a sufficient distance between the two. The batteries for mobile units in MIMO systems last less time than those in single-input, single-output (SISO) systems, and thus use more power. Since ST and STF encoder and decoder involve sophisticated calculations, MIMO transceivers need a powerful DSP unit.

In this research, we provide a novel diversity method for SISO spread spectrum systems that, although using just one transmitting and one receiving antenna, may achieve a diversity gain comparable to that of the MIMO system. With two degrees of freedom (the number of transmitting and receiving antennas), the MIMO system provides diversity gain. There is also a diversity gain with two degrees of freedom in the suggested diversity scheme. While the suggested system only has one transmitting antenna and one receiving antenna, the diversity gain is achieved by employing N spreading codes and L uncorrelated propagation pathways. Code-time variety is covered in further depth in Section 2. The signal model and the new transmit diversity method are shown in Section 3.

The encoded data symbol is broadcast multiple times over various symbol periods utilising various transmitting antennas in a space-time MIMO system. The received symbol might have independent fading gains due to the transmission of the symbols across separate time slots. It is far less likely to get the sent symbol with fading gains across subsequent time periods. Moreover, the use of many antennas enables the broadcast symbol to have separate fading gains across each route as well as independent propagation pathways from the transmitter to the receiver. Hence, the various time slots and propagation routes are what primarily contribute to the improvement of the diversity gain of the time-space MIMO system [10] .

We use the same idea of time and space diversities in the suggested code-time diversity approach, but via a different process. The current data symbol and the preceding (N1) ones are spread apart in frequency throughout each symbol period utilising N separate spreading code sequences for each data symbol. A collection of N orthogonal codes is utilised to create the spreading codes. Using a single antenna, the scattered symbols are combined and sent. The employed spreading sequences' orthogonality avoids interference between the transmitted signals. At each symbol period, the same process is repeated in order to broadcast each signal N times through N subsequent symbol periods, each time using a different spreading code from the set of N orthogonal codes. Three separate orthogonal spreading codes are used to broadcast the modulated data symbols three times at three subsequent symbol periods. By doing this, temporal variety is established and there is a far lower chance of N fading gains occurring during N consecutive symbol periods.

By adjusting the scattered symbols' bandwidth to be bigger than the wireless channel's coherent bandwidth, spatial diversity is made possible. Uncorrelated multipath propagation between the transmitter and receiver is made possible by this. The information message bandwidth is increased by employing direct sequence spread spectrum (DSSS) by a factor equal to the spreading process gain, which is equal to the ratio between the data symbol period and the spreading code chip period. It is possible to equalise the spread signal's bandwidth by adjusting

the process gain. The code-time diversity DSSS modulator, can modulate signals at multiples of the channel's coherent bandwidth. L=Bandwidth of DSSS signal Channel coherent bandwidth + 0.5 gives the potential number of uncorrelated pathways from the transmitter to the receiver. In a similar manner, there is a large decrease in the likelihood of spatial gains that fade across the uncorrelated propagation pathways L. The suggested code-time diversity system offers the same diversity gain as the space-time MIMO system with two degrees of freedom. While the number of antennas in the transmitter Nt and receiver Nr determine the diversity gain in a time-space MIMO system, the number of spreading codes N (which corresponds to the number of time slots through which each symbol will be repeated) and the number of uncorrelated propagation paths L determine the diversity gain in a code-time diversity system.

The transmitter and receiver of the suggested diversity system each include a single antenna and RF interface device. The code-time diversity employs a spread signal with a greater bandwidth than the transmitted signal in the time-space MIMO system, yet it seems to have a diversity gain comparable to that of the time-space MIMO system. In other words, the cost of improving the diversity gain utilising a streamlined hardware of a single antenna and a single RF interface in the transmitter and in the receiver is the increase in the signal bandwidth of the proposed code-time diversity system. The orthogonality between the spreading codes is the sole need for the code-time. The Scientific World Journal made the following assumptions in the case when the fading gain is constant for one symbol period and varies arbitrarily from symbol to symbol: Gaussian random variable having a mean of zero and a variation of two the sent signal moves over unresolvable propagation channels from the transmitter to the receiver in a flat fading channel. As a result, the signal's frequency components will all fade to the same degree. The flat fading situation in our suggested diversity scheme resembles the MISO system, where a single antenna at the receiver receives the modulated symbols that are sent by several antennas.

Our signal model states that the received signal at the demodulator input is represented by the formula r (t) = K1 k=0 N1 n=0 kdkncn (t kTs) + w (t), where w(t) is a sample function of a white Gaussian noise process with zero mean and 2 w variance. During the kth symbol period, k is the channel random gain. Three components make up the proposed demodulator for the code-time diversity system. A bank of correlators in the first section correlates the incoming signal with the N spreading codes. Over one symbol period, the nth correlator compares the received signal to the nth spreading code, cn(t). The output of the nth correlator during the kth symbol period is seen in (9a) and (9b):

The combined signals in are equal to those of an MRC receiver with an N-branch. The novel code-time diversity technique, which uses N spreading orthogonal codes and a single transmission antenna, produces the same diversity order as the N-branch MRC receiver scheme. The combined signals in are comparable to those of a space-time MIMO system with N antennas at the transmitter and one antenna at the receiver or a space-time MIMO system with one antenna at the transmitter and N antennas at the receiver, it is crucial to note. In contrast to the spacetime encoder and decoder in the space-time MIMO system, the proposed codetime diversity system does not employ extra encoders or decoders at the transmitter or the receiver.

In the code-time diversity, no extra RF interface circuits or antennas are needed. Circuits for spreading and dispersing are the only extra components utilised. The longer bandwidth and N symbol period delays that come before the first sent signal's detection are disadvantages of the proposed code-time diversity scheme. The decision variable is initially computed in the proposed

code-time diversity system to estimate the chance of symbol mistake. The Scientific World Journal's optimal detector determines the choice variable by multiplying the signal in by the conjugate of all the complex symbols.

The generalised hyper-geometric function is called pFq. Restrictions on the Spreading Codes in Use. The suggested code-time diversity system uses DSSS, which increases the sent signal bandwidth beyond that of the nonspread modulated symbols and beyond that of the broadcast signal if a space-time coding MIMO system is used. While the code-time diversity system's expanded bandwidth boosts channel capacity and strengthens the system's susceptibility to jamming and interference signals, its bandwidth efficiency remains subpar. More than one user may use a separate set of orthogonal spreading codes while still sharing the same channel bandwidth in a codetime diversity system to improve bandwidth efficiency. The suggested diversity system requires MN orthogonal spreading codes if M users share the same channel. This puts more pressure on orthogonal spreading codes.

The employment of a multiuser DSSS system with code-time diversity improves the system's bandwidth efficiency, however in this situation, a multiuser detector should be employed in the receiver rather than a single user detector[11]. We will go into more depth on this topic in a later study, but for now, let's stick with the single user detector situation. It assume that the N spreading codes being employed are mutually orthogonal, illustrate the likelihood of error and the average probability of error in the received data for the cases of nonfaded and faded channels, respectively. On the other hand, the correlation between the code pairings impacts the likelihood of mistake when nonorthogonal codes, such as a PN sequence and its cyclic shifted sequences, are utilised. Intersymbol interference (ISI) between the transmitted signals is caused by this correlation.

CONCLUSION

Spread spectrum is a key technique used in modern communication systems to improve the reliability, security, and capacity of wireless networks. This technique spreads the signal over a wider frequency band than is necessary for transmission, making it more resistant to interference and eavesdropping. Spread spectrum has several variants, including direct sequence spread spectrum (DSSS) and frequency hopping spread spectrum (FHSS), each with its own advantages and limitations. DSSS uses a high data rate and a pseudo-random sequence to spread the signal over a wide frequency band, while FHSS rapidly hops between different frequency channels to avoid interference and improve security.

REFERENCES

[1] X. Wang and C. Caloz, “Spread-Spectrum Selective Camouflaging Based on Time-Modulated Metasurface,” *IEEE Trans. Antennas Propag.*, 2021, doi: 10.1109/ TAP.2020.3008621.

[2] S. H. Soleymani and A. H. Taherinia, “Double expanding robust image watermarking based on Spread Spectrum technique and BCH coding,” *Multimed. Tools Appl.*, 2017, doi: 10.1007/s11042-016-3734-2.

[3] W. Zhang, B. Zhang, and F. Zhou, “Space–time receiver for spread spectrum communication systems with beam tracking,” *IET Radar, Sonar Navig.*, 2022, doi: 10.1049/rsn2.12230.

[4] P. Čisar, P. Odry, S. Maravić Čisar, and G. Stankov, "Teaching spread spectrum in the course Telecommunication Systems using Octave," *Comput. Appl. Eng. Educ.*, 2020, doi: 10.1002/cae.22199.

[5] Y. Zhang, Z. Xu, and B. Huang, "Channel capacity analysis of the generalized spread spectrum watermarking in audio signals," *IEEE Signal Process. Lett.*, 2015, doi: 10.1109/LSP.2014.2363655.

[6] M. Li, X. Xi, X. Zhang, and G. Liu, "Joint Compressed Sensing and Spread Spectrum Through-the-Wall Radar Imaging," *IEEE Access*, 2021, doi: 10.1109/ACCESS. 2020.3048184.

[7] S. Luo, S. Zhang, S. Ke, S. Wang, X. Bu, and J. An, "Optimum Combining for Coherent FFH/DS Spread Spectrum Receivers in the Presence of Multi-Tone Jammer," *IEEE Access*, 2020, doi: 10.1109/ACCESS.2020.2980858.

[8] X. S. Zhu, Y. Sun, Q. H. Meng, B. Sun, P. Wang, and T. Yang, "Optimal watermark embedding combining spread spectrum and quantization," *EURASIP J. Adv. Signal Process.*, 2016, doi: 10.1186/s13634-016-0373-8.

[9] A. J. Suzuki, M. Yamamoto, and K. Mizui, "Visible light V2V communication and ranging system prototypes using spread spectrum techniques," *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.*, 2020, doi: 10.1587/transfun.2019TSP0004.

[10] A. Rodríguez-Martínez *et al.*, "On the Optimization of Spread Spectrum Chirps into Arbitrary Position and Width Pulse Signals. Application to Ultrasonic Sensors and Systems," *IEEE Access*, 2022, doi: 10.1109/ACCESS.2021.3139562.

[11] D. Kirovski and H. S. Malvar, "Spread-spectrum watermarking of audio signals," *IEEE Trans. Signal Process.*, 2003, doi: 10.1109/TSP.2003.809384.

CHAPTER 22

CIRCUIT SWITCHING AND PACKET SWITCHING: A COMPARATIVE ANALYSIS OF TECHNIQUES FOR RELIABLE AND EFFICIENT DATA COMMUNICATION NETWORKS

Alka Verma, Associate Professor
Department of Electronics and Communication Engineering,
Teerthanker Mahaveer University, Moradabad, Uttar Pradesh, India
Email Id- alkasinghmail@rediffmail.com

ABSTRACT:

Circuit switching and packet switching are two fundamental technologies used in modern telecommunications and computer networks to transfer data between devices. Circuit switching establishes a dedicated physical path between two devices before data transmission, while packet switching breaks the data into smaller packets and sends them separately over the network. The circuit is set up by the telephone exchange, which is a central node in the network that connects different circuits together. The exchange receives the call request, checks if the destination is available, and if it is, the exchange sets up a dedicated circuit for the call. The exchange keeps the circuit open until the conversation is finished, after which it releases the circuit for other calls.

KEYWORDS:

Circuit, Data Transmission, Packet Switching, Telecommunication, Switching.

INTRODUCTION

Circuit switching and packet switching are two important technologies that are used to manage communication networks. While circuit switching was the traditional method used in the early days of communication networks, packet switching has become more popular in recent years due to its efficiency and flexibility. In this essay, we will explore the differences between these two methods of communication, their strengths and weaknesses, and how they are used in modern communication networks [1]–[3].

Circuit Switching

Circuit switching is a method of communication that was used in the early days of telephone networks. In this system, a physical connection is established between two parties, and this connection is maintained for the duration of the conversation. This connection is called a circuit, and it is dedicated to that particular communication. When a user wants to make a call, they dial the phone number of the person they wish to speak to, and the system connects them via a circuit.

Circuit switching is a reliable and secure method of communication. Since the circuit is dedicated to a particular conversation, there is no risk of interference from other calls. The quality of the connection is also high, as there is no delay or loss of data due to congestion. However, this method is inefficient since the circuit is dedicated to a single conversation, which

means that it is not being used when there is no conversation. This means that a significant portion of the network capacity is wasted.

Packet Switching

Packet switching is a more recent method of communication that is used in modern communication networks such as the internet. In this system, data is split into small packets, which are then sent across the network. Each packet contains a header that contains the destination address, the source address, and other information. The packets are sent across the network independently and are reassembled at the destination [4], [5].

Packet switching allows multiple users to share a single connection, making it much more efficient than circuit switching. It also allows for more flexibility in communication since packets can be sent in any order and can take different paths across the network. If a particular path is congested, packets can be rerouted through an alternative path, which ensures that the network always operates at peak efficiency.

One of the main advantages of packet switching is that it allows for more efficient use of network resources. Since packets are sent independently, the network can use the available capacity more efficiently, and there is less waste. Packet switching is also more flexible than circuit switching since packets can take different paths and be sent in any order. This means that the network can adapt to changing conditions and can route traffic around congested areas.

However, packet switching is not as reliable as circuit switching since there is a risk of packet loss or delay. Packets can be lost due to network congestion or other issues, which can result in data loss or corruption. This can be mitigated by implementing error-checking and recovery mechanisms, but these add complexity to the network and can reduce efficiency.

Comparison

Circuit switching and packet switching are two very different methods of communication, and each has its strengths and weaknesses. Circuit switching is a reliable and secure method of communication that is suitable for voice communication, but it is inefficient and not well-suited to modern data communication. Packet switching, on the other hand, is a more efficient and flexible method of communication that is well-suited to data communication but is less reliable than circuit switching.

One of the main differences between circuit switching and packet switching is the way that the network capacity is used. In circuit switching, the capacity is dedicated to a particular conversation and is not available for other conversations until the circuit is released. This means that a significant portion of the network capacity is wasted when no conversation is taking place. In contrast, packet switching allows multiple users to share a single connection, making it much more efficient than circuit switching. This allows the network to use the available capacity more efficiently and reduces waste [6].

Another difference between circuit switching and packet switching is the way that they handle congestion. In circuit switching, if there is congestion in the network, the call request is either delayed or dropped. This can result in a poor user experience and can be frustrating for users. In contrast, packet switching can handle congestion more efficiently by rerouting packets around

congested areas. This ensures that the network always operates at peak efficiency, and there is less risk of delays or dropped packets.

One of the strengths of circuit switching is its reliability and security. Since the circuit is dedicated to a particular conversation, there is no risk of interference from other conversations. This makes circuit switching ideal for voice communication, where it is important to ensure that the conversation is private and secure. However, this reliability comes at a cost, as circuit switching is not well-suited to modern data communication.

DISCUSSION

Packet switching, on the other hand, is well-suited to modern data communication. Since packets can be sent independently and take different paths across the network, packet switching allows for more efficient use of network resources and greater flexibility in communication. However, packet switching is not as reliable as circuit switching, and there is a risk of packet loss or delay. This can be mitigated by implementing error-checking and recovery mechanisms, but these can add complexity to the network and reduce efficiency.

Both circuit switching and packet switching are used in modern communication networks. Circuit switching is still used for voice communication, particularly in traditional telephone networks. However, in modern data communication networks, packet switching is the preferred method of communication. The internet, for example, is a packet-switched network, and most data communication today is conducted using packet switching.

In modern communication networks, packet switching is used to transport data across the network, while circuit switching is used for control and signaling. For example, in a telephone network, circuit switching is used to set up and release voice circuits, while packet switching is used to transport data between users circuit switching and packet switching are two important methods of communication that have been used in communication networks for many years. Circuit switching is a reliable and secure method of communication that is suitable for voice communication, but it is inefficient and not well-suited to modern data communication.

Packet switching, on the other hand, is a more efficient and flexible method of communication that is well-suited to data communication but is less reliable than circuit switching. In modern communication networks, packet switching is the preferred method of communication for data communication, while circuit switching is still used for voice communication. The use of these technologies depends on the requirements of the particular communication network, and the choice of technology depends on the specific needs of the users. To further understand the differences between circuit switching and packet switching, it's important to explore the technical details of each method.

In circuit switching, a connection is established between the sender and the receiver, and a dedicated circuit is created for the duration of the communication. The circuit provides a direct path for the transmission of data, and it remains dedicated to the conversation until it is released. The circuit-switched network is designed to ensure a stable connection for the duration of the communication.

During the call setup phase, a path is established between the sender and the receiver by reserving the necessary resources, such as bandwidth, for the call. In this phase, data is

transmitted over the dedicated circuit from the sender to the receiver. Once the communication is completed, the circuit is released and the resources are returned to the network.

Circuit switching requires more infrastructure to be in place for a connection to be established, and it requires that the network capacity is reserved for the entire duration of the communication, even when there is no data transmission. This results in a lower efficiency of network utilization, but it ensures a stable connection that is ideal for real-time voice communication. In packet switching, data is divided into small packets, which are sent over the network independently. Each packet contains information about the sender, receiver, and the data itself. These packets are sent over the network through different routes and can be reassembled at the destination.

Packet switching is more flexible than circuit switching, as it allows for efficient utilization of network resources. Multiple users can share the same network resources, which makes packet switching more efficient for data communication. However, it is less reliable than circuit switching, and there is a risk of packet loss or delay. To address this issue, packet switching networks use error-checking and recovery mechanisms, such as TCP (Transmission Control Protocol), to ensure the integrity of the data.

In summary, circuit switching and packet switching are two different methods of communication that have their strengths and weaknesses. Circuit switching is ideal for voice communication, while packet switching is ideal for data communication. The choice of technology depends on the specific needs of the users and the network. Communication networks typically use both technologies in different parts of the network, depending on the requirements [7]. In addition to the technical differences, there are other factors that differentiate circuit switching and packet switching, such as cost and scalability.

Circuit switching is more expensive than packet switching because it requires the reservation of dedicated resources, such as bandwidth, for the entire duration of the communication, regardless of whether or not data is being transmitted. This results in an inefficient use of network resources, which drives up the cost. Packet switching, on the other hand, is more cost-effective because it allows multiple users to share the same network resources. This enables a more efficient use of network resources and reduces the overall cost of the network.

Packet switching is more scalable than circuit switching. In a circuit-switched network, the resources must be reserved for the entire duration of the communication, which limits the number of concurrent connections that can be supported. As a result, circuit-switched networks are not scalable, and they become congested when the number of users increases. In contrast, packet switching allows multiple users to share the same network resources. This makes packet switching more scalable than circuit switching, as it can handle a large number of users without becoming congested.

Circuit switching is typically used for real-time communication, such as voice and video communication. It provides a stable and reliable connection that is necessary for these applications. Packet switching is used for data communication, such as email, web browsing, and file transfer. It is also used for real-time applications, such as video conferencing, but it requires the use of additional mechanisms, such as Quality of Service (QoS), to ensure that the data is delivered in a timely manner.

Circuit switching and packet switching are two different methods of communication that are used in modern networks. Circuit switching is ideal for real-time voice communication, while packet switching is ideal for data communication. The choice of technology depends on the specific needs of the users and the network. Communication networks typically use both technologies in different parts of the network, depending on the requirements. Ultimately, the choice of technology depends on factors such as cost, scalability, and application requirements.

Circuit switching and packet switching are two different methods used for transmitting data over a communication network. These methods are used to establish communication channels between two devices or nodes in a network. In this article, we will discuss circuit switching and packet switching in detail, their characteristics, advantages, disadvantages, and the applications where they are used. Circuit switching is a technique used in communication networks to establish a dedicated communication path between two devices or nodes in a network. In circuit switching, a dedicated communication path is established between the two devices for the entire duration of the communication. The communication path remains reserved for the entire time, even if no data is being transmitted.

The circuit switching process is initiated when a user dials a number or sends a request to connect to another device. The network establishes a dedicated communication path between the two devices by reserving the required resources, such as bandwidth and processing power, for the entire duration of the communication. The communication path is released after the communication is completed or terminated[8], [9] . Circuit switching is commonly used in telephone networks, where a dedicated communication path is established between two devices for the entire duration of the call. The resources required for the communication are reserved in advance, which ensures a consistent quality of service throughout the communication. The communication path remains dedicated, which means that the bandwidth is not shared with any other communication. As a result, circuit switching offers a reliable, predictable, and consistent communication service.

However, circuit switching has certain limitations. Since the communication path remains reserved for the entire duration of the communication, even if no data is being transmitted, circuit switching is not an efficient method for transmitting small amounts of data. The resources required for the communication are not utilized optimally, which can result in wastage of resources. Packet switching is a technique used in communication networks to transmit data by dividing it into small, fixed-sized packets. The packets are then transmitted over the network to the destination device or node. In packet switching, the packets are transmitted independently and can take different paths to reach the destination. The packet switching process begins when a user sends a request to transmit data. The data is divided into small packets, each with a fixed size. Each packet is then transmitted independently over the network. The packets can take different paths to reach the destination, and they can arrive at different times. The packets are then reassembled at the destination device to form the original data.

Packet switching is commonly used in computer networks and the internet. In packet switching, the resources required for the communication are shared among multiple communications, which makes it an efficient method for transmitting small amounts of data. Since the packets can take different paths to reach the destination, packet switching offers a robust communication service that can handle network congestion and failures. Packet switching offers several advantages over circuit switching. Since the resources required for the communication are shared among multiple

communications, packet switching is an efficient method for transmitting small amounts of data. Packet switching also offers a robust communication service that can handle network congestion and failures. If a packet is lost or delayed, it can be retransmitted, which ensures reliable communication.

However, packet switching also has certain limitations. The packets can arrive at different times, which can result in delays in reassembling the original data. Packet switching also does not offer a consistent quality of service, as the bandwidth is shared among multiple communications. As a result, the quality of service can vary depending on the network congestion and the number of users. In circuit switching, the resources required for the communication are reserved and dedicated for the entire duration of the communication. In packet switching, the resources required for the communication are shared among multiple communications. Circuit switching offers a consistent and predictable quality of service throughout the communication. Packet switching does not offer a consistent quality of service, as the bandwidth is shared among multiple communications.

Packet switching is more efficient for transmitting small amounts of data, as the resources required for the communication are shared among multiple communications. Circuit switching is less efficient for transmitting small amounts of data, as the resources required for the communication are reserved for the entire duration of the communication. Packet switching is more robust and fault-tolerant than circuit switching. In packet switching, the packets can take different paths to reach the destination, which makes it robust against network congestion and failures. In circuit switching, the communication path remains dedicated, which makes it vulnerable to network congestion and failures. Circuit switching is more expensive than packet switching, as the resources required for the communication are reserved for the entire duration of the communication. Packet switching is less expensive than circuit switching, as the resources required for the communication are shared among multiple communications.

Circuit switching is commonly used in telephone networks, where a dedicated communication path is established between two devices for the entire duration of the call. The resources required for the communication are reserved in advance, which ensures a consistent quality of service throughout the communication.Packet switching is commonly used in data networks, such as the internet, where data is transmitted in the form of small packets. The packets are transmitted independently and can take different paths to reach the destination. Packet switching offers an efficient and robust method for transmitting small amounts of data.

Circuit switching is commonly used in multimedia applications, such as video conferencing and streaming, where a consistent quality of service is required. Packet switching can be used in multimedia applications, but it requires a mechanism for ensuring a consistent quality of service, such as Quality of Service (QoS) mechanisms.Circuit switching is commonly used in military communications, where a dedicated and secure communication path is required. Packet switching can also be used in military communications, but it requires encryption and other security mechanisms to ensure the confidentiality and integrity of the data.

Circuit switching is commonly used in financial transactions, such as credit card transactions, where a reliable and secure communication path is required. Packet switching can also be used in financial transactions, but it requires encryption and other security mechanisms to ensure the confidentiality and integrity of the data.Circuit switching and packet switching are two different methods used for transmitting data over a communication network. Circuit switching offers a

dedicated and reliable communication path, but it is less efficient for transmitting small amounts of data. Packet switching offers an efficient and robust method for transmitting small amounts of data, but it does not offer a consistent quality of service. The choice between circuit switching and packet switching depends on the application requirements and the trade-offs between the characteristics, advantages, and disadvantages of each method.

Circuit switching is a method of transmitting data over a communication network by establishing a dedicated communication path between two devices for the entire duration of the communication. The resources required for the communication, such as bandwidth and memory, are reserved in advance and remain dedicated for the entire duration of the communication. Circuit switching was the dominant method of transmitting data in the early days of telecommunication, such as in the telephone network. In the telephone network, a circuit is established between two devices for the entire duration of the call. The resources required for the communication, such as bandwidth and memory, are reserved in advance and remain dedicated for the entire duration of the call. This ensures a consistent and predictable quality of service throughout the communication.

Circuit switching has several advantages, such as a consistent and predictable quality of service throughout the communication, a secure and dedicated communication path, and a low latency. However, circuit switching also has several disadvantages, such as inefficiency for transmitting small amounts of data, vulnerability to network congestion and failures, and high cost. Packet switching is a method of transmitting data over a communication network by dividing the data into small packets and transmitting them independently. The packets can take different paths to reach the destination, and they are reassembled into the original data at the destination.

Packet switching was developed in the 1960s as a more efficient method of transmitting data over a communication network. In packet switching, the resources required for the communication are shared among multiple communications, which makes it more efficient for transmitting small amounts of data. Packet switching also offers a more robust and fault-tolerant method of transmitting data, as the packets can take different paths to reach the destination and are not vulnerable to network congestion and failures [10] .

Packet switching has several advantages, such as efficiency for transmitting small amounts of data, robustness and fault-tolerance, and low cost. However, packet switching also has several disadvantages, such as a lack of a consistent and predictable quality of service, vulnerability to packet loss and delay, and the need for a mechanism to ensure a consistent quality of service. The Internet uses packet switching as its primary method of transmitting data. In the Internet, data is transmitted in the form of small packets that can take different paths to reach the destination. This makes the Internet a highly efficient and resilient communication network, as it can handle large amounts of data and is not vulnerable to network congestion and failures.

However, the lack of a consistent and predictable quality of service in packet switching can be a problem for certain applications that require a high-quality and reliable communication channel, such as voice and video conferencing. To address this issue, various mechanisms have been developed to provide a consistent quality of service in the Internet, such as Differentiated Services (DiffServ) and Resource Reservation Protocol (RSVP).

DiffServ is a mechanism for providing a differentiated quality of service in the Internet, where packets are classified into different traffic classes based on their importance and priority. The

network can then prioritize the traffic based on the traffic class and ensure a consistent quality of service for each traffic class. RSVP is a protocol for reserving network resources for a specific communication session in advance. This allows the network to provide a consistent quality of service for the entire duration of the communication session, similar to circuit switching. However, RSVP is not widely used in the Internet due to its complexity and scalability issues.

Another approach to providing a consistent quality of service in the Internet is to use a hybrid approach that combines circuit switching and packet switching. This approach, known as Virtual Circuit (VC) or Connection-Oriented Packet Switching, establishes a virtual circuit between two devices for the entire duration of the communication, similar to circuit switching. However, the communication is still transmitted in the form of packets, which makes it more efficient and resilient than circuit switching[11]. The lack of a consistent and predictable quality of service in packet switching can be a problem for certain applications that require a high-quality and reliable communication channel. Various mechanisms, such as DiffServ and RSVP, have been developed to address this issue both circuit switching and packet switching have their advantages and disadvantages, and the choice between them depends on the specific requirements of the communication. Circuit switching is best suited for applications that require a consistent and predictable quality of service, while packet switching is best suited for applications that require efficiency and resilience.

CONCLUSION

Circuit switching and packet switching are two different methods of transmitting data over a communication network. Circuit switching is a method of transmitting data by establishing a dedicated communication path between two devices for the entire duration of the communication, while packet switching is a method of transmitting data by dividing the data into small packets and transmitting them independently. Packet switching is the primary method of transmitting data in the Internet, as it is more efficient and resilient than circuit switching.

REFERENCES

[1] M. Sneps-Sneppe, “Circuit Switching versus Packet Switching,” *Int. J. Open Inf. Technol.*, 2015.

[2] A. K. Lusala and J. D. Legat, “Combining SDM-based circuit switching with packet switching in a router for on-chip networks,” *Int. J. Reconfigurable Comput.*, 2012, doi: 10.1155/2012/474765.

[3] R. Stabile, A. Albores-Mejia, A. Rohit, and K. A. Williams, “Integrated optical switch matrices for packet data networks,” *Microsystems and Nanoengineering*. 2016. doi: 10.1038/micronano.2015.42.

[4] P. Andreades, K. Clark, P. M. Watts, and G. Zervas, “Experimental demonstration of an ultra-low latency control plane for optical packet switching in data center networks,” *Opt. Switch. Netw.*, 2019, doi: 10.1016/j.osn.2018.11.005.

[5] G. Retske, “Packet Switching vs. Circuit Switching,” in *A Guide to Competitive International Telecommunications*, 2020. doi: 10.1201/9781482280708-28.

[6] T. N. Truong and R. Takano, “Hybrid electrical/optical switch architectures for training distributed deep learning in large-scale,” *IEICE Trans. Inf. Syst.*, 2021, doi: 10.1587/transinf.2020EDP7201.

[7] K. I. Kitayama *et al.*, “Torus-topology data center network based on optical packet/agile circuit switching with intelligent flow management,” *J. Light. Technol.*, 2015, doi: 10.1109/JLT.2015.2394384.

[8] S. J. B. Yoo, “Optical packet and burst switching technologies for the future photonic internet,” *Journal of Lightwave Technology*. 2006. doi: 10.1109/JLT.2006.886060.

[9] A. S. Raja *et al.*, “Ultrafast optical circuit switching for data centers using integrated soliton microcombs,” *Nat. Commun.*, 2021, doi: 10.1038/s41467-021-25841-8.

[10] M. A. Schneps-Schneppe, “Circuit switching is coming back?,” *Autom. Control Comput. Sci.*, 2015, doi: 10.3103/S0146411615010083.

[11] L. G. Roberts, “The Evolution of Packet Switching,” *Proc. IEEE*, 1978, doi: 10.1109/PROC.1978.11141.

CHAPTER 23

ASYNCHRONOUS TRANSFER MODE (ATM): ARCHITECTURE, PROTOCOLS, AND APPLICATIONS IN MODERN COMMUNICATION NETWORKS

Prashant Kumar, Assistant Professor
Department of Electronics and Communication Engineering,
Teerthanker Mahaveer University, Moradabad, Uttar Pradesh, India
Email Id- tmu.iqac@gmail.com

ABSTRACT:

Asynchronous Transfer Mode (ATM) is a high-speed networking technology that is designed to efficiently handle voice, data, and video traffic in a single network. ATM networks use fixed-length cells to transmit data, which allows for fast and efficient processing of data and supports high data rates of up to 622 Mbps. ATM is based on a virtual circuit switching approach, where a virtual circuit is established between two devices for the duration of a communication session. The virtual circuit allows for the efficient transmission of data, as the network can reserve resources in advance and ensure a consistent quality of service for the entire communication session.

KEYWORDS:

Asynchronous Transfer, Communication, Network, Voice Data, Video Traffic.

INTRODUCTION

An efficient packet transmission interface is ATM. Cells, which are fixed-size packets used by ATM, One effective method for transmission over high-speed networks is to employ a set size and defined format. ATM cells must be transported via some kind of transmission structure. The employment of a continuous stream of cells without imposing a multiplex frame structure at the interface is one possibility. The process of synchronization occurs cell by cell. The cells might also be arranged in a synchronous time-division multiplex envelope as a second alternative. In this instance, the external frame of the bit stream at the interface is based on the Synchronous Digital Hierarchy (SDH). Both real-time and non-real-time services are offered by ATM [1]–[3].

An ATM-based network can handle a variety of traffic types, including synchronous TDM streams like T-1, which use the constant bit rate (CBR) service; compressed voice and video, which use the real-time variable bit rate (rt-VBR) service; traffic with specific quality-of-service requirements, which use the non-real-time VBR (nrt-VBR) service; and IP-based traffic, which uses the available bit rate (ABR), unspecified bit rate (UBR

Asynchronous transfer mode (ATM), often known as cell relay, provides quicker packet switching than X.25 by using the dependability and integrity of contemporary digital infrastructure. Asynchronous transfer mode has some similarities with frame relay and X.25-based packet switching. A similar to frame relay and packet switching, ATM includes the transport of data in discrete chunks. Moreover, ATM enables numerous logical connections to be multiplexed over a single physical interface, much as packet switching and frame relay [4].

A simplified protocol with little room for mistake and good flow control skills is ATM. As a result, ATM may run at high data rates with less overhead associated with processing ATM cells and fewer overhead bits needed for each cell. Another factor encouraging the usage of ATM at high data rates is the use of fixed-size cells, which makes the processing necessary at each ATM node simpler. ITU-ATM T's standards are based on the protocol architecture, which shows the fundamental design of a user-network interface. The definition of a transmission medium and a signal encoding strategy takes place at the physical layer. The physical layer's defined data speeds vary from 25.6 Mbps to 622.08 Mbps. It's possible to use different data rates, both greater and lower.

The protocol design has two levels that are related to ATM operations. There is an ATM layer that is shared by all services and allows for packet transmission, as well as an ATM adaption layer (AAL) that is service-specific. The utilisation of logical connections and the transfer of data in fixed-size cells are both defined by the ATM layer. When ATM is used, an adaption layer is required to allow information transfer protocols that aren't ATM-based. The AAL takes information from ATM cells and delivers it to higher levels by mapping information from higher layers into ATM cells for transit via an ATM network.

Three different planes are included in the protocol reference model:

a) **Control Plane:**Executes call control and connection control operations.
b) **User Plane:**Allows for the transmission of user information and any related controls (e.g., flow control, error control).
c) **Management Plane:**Consists of layer management, which manages the resources and parameters found in its protocol entities, and plane management, which manages the system as a whole and facilitates coordination across all the planes.

A VCC is the fundamental switching element of an ATM network and is comparable to an X.25 virtual circuit. Via the network, a Link is established between two end users, and over that connection, a variable-rate, full-duplex flow of fixed-size cells is sent. VCCs are also used for network-to-network and user-to-network communication (control signalling) (network management and routing).

For ATM, a second sublayer of processing that deals with the idea of virtual paths has been implemented. The term "virtual path connection" (VPC) refers to a collection of VCCs with the same endpoints. As a result, every cell running through every VCC in a single VPC is switched at the same time. In response to a tendency in high-speed networking where the control cost of the network is becoming an ever larger fraction of the total network cost, the virtual route idea was created. The virtual route approach reduces the control cost by combining connections that go along similar pathways in the network. Hence, rather of managing a large number of individual connections, network management operations may be performed to a limited number of groups of connections. Network transport functions may be divided into those connected to a single logical connection (virtual channel) and those related to a collection of logical connections, resulting in a more straightforward network design (virtual path)[5], [6]. When fewer, aggregated entities are dealt with by the network, performance and reliability have increased.

Faster connection setup and decreased processing time: Most of the work is completed when the virtual link is established. New virtual channel connections may be formed by performing basic

control functions at the endpoints of a virtual route connection in anticipation of further call arrivals; no call processing is required at transit nodes the work required to add additional virtual channels to an existing virtual route is thus low. Improved network services: While utilised internally by the network, the virtual route is also accessible to end users. As a result, the user may create closed networks of virtual channel bundles or user groups.

Virtual path management techniques include calculating routes, assigning capacity, and storing connection status data. The process of establishing up a virtual path connection is separated from the process of setting up a specific virtual channel connection. Before creating a virtual channel, a virtual route connection to the desired destination node must be established. This connection must have sufficient capacity and the right quality of service to enable the virtual channel. By saving the necessary state data (virtual channel/virtual route mapping), a virtual channel is created.

Between the point where a VCI value is assigned and the point where that value is translated or terminated, there is a way to transport ATM cells unidirectional via a virtual channel link. Identifier for a virtual channel a special number tag that designates a specific VC connection for a certain (VCI) VPC. Connection to a virtual channel a grouping of VC connections that connects two locations where users of the ATM (VCC) service may access the ATM layer. VCCs are made available for the flow of information between users, networks, or networks of users.

DISCUSSION

Virtual Route a general name for the unidirectional transfer of ATM cells that are a part of virtual channels and connected by a single, shared unique identification value. A set of VC connections between the point where a VPI value is assigned and the point where that value is translated or terminated is referred to as a virtual path link. A specific VP connection is identified by a virtual path identifier (VPI). A concatenation of VP connections known as a virtual path connection (VPC) increases the length of a group of VC links that share the same VPI. It occurs between the point when the VCI values are assigned and the point where those values are translated or withdrawn. VPCs are made available for the exchange of information between users, networks, or networks themselves.

The standard's vocabulary for virtual pathways and virtual channels, which is a little difficult to understand, is compiled. The concepts of virtual path and virtual channel are defined in the ITU-T Recommendations with reference to both the user-network interface and the internal network operation, in contrast to the majority of the network-layer protocols that we deal with in this book that relate only to the user-network interface. A VCC may have end users, network entities, or both end users and network entities as its endpoints. Cell sequence integrity is always maintained inside a VCC, meaning that cells are always delivered in the same order that they were supplied. Let's look at some instances of the three applications of a VCC:

Between end users: May be used to transmit end-to-end user data; can also be used, as will be discussed later, to transmit control signals between end users. A VPC between end users gives them a total capacity; the two end users may decide how the VPC is organised as long as the total number of VCCs does not go above the VPC capacity [7] . Between two entities in a network: used for routing and managing network traffic. A common pathway for the sharing of network management information may be established via a network-to-network VPC.

Average rate, peak rate, burstiness, and peak duration are the several traffic parameter categories that may be agreed upon. To manage current and requested VCCs and cope with congestion, the network may require a multitude of techniques. In its most basic form, the network may only reject further requests for VCCs to avoid congestion. Moreover, if agreed parameters are broken or there is a lot of congestion, cells could be rejected. Existing connections could be severed in certain circumstances [8] . The first four qualities are exactly the same as for VCCs. In other words, a VPC also has QoS, switched and semipermanent VPCs, cell sequence integrity, traffic parameter negotiation, and use monitoring. This duplication is happening for a variety of reasons.

First off, it gives the network provider considerable latitude in how it handles the demands imposed on it. A VPC's overall needs must be a concern for the network, and inside a VPC, it is possible to negotiate the creation of virtual channels with certain properties. Lastly, when a VPC has been established, end users may bargain for the development of additional VCCs. The end users' potential choices are limited by the VPC features. Virtual channel identifier restrictions inside a VPC: The user of the VPC may not have access to one or more virtual channel IDs, or numbers, which may be restricted for network usage. Examples are network management VCCs.

The construction and release of VPCs and VCCs in ATM need a method. Control signalling, the information exchange involved in this process, takes occur on connections apart from those that are being monitored. A call control signalling channel must be created if there isn't already one. A control signalling exchange between the user and the network must happen on some channel in order to do that. So, we need a permanent channel that can be used to establish VCCs that can be used for call control and is most likely to have a modest data rate. A channel like this is known as a meta-signaling channel since it is used to configure other signalling channels.

A VCC may be established between the user and the network for call control signalling using the meta-signaling channel. The establishment of VCCs to convey user data may then be done via this user-to-network signalling virtual channel. A user-to-user signalling virtual channel may also be established using the meta-signaling channel. An existing VPC must be used to set up such a channel. The two end users may then utilise it to create and release user-to-user VCCs to transfer user data without the need for network involvement.

A 5-octet header and a 48-octet information field make up the fixed-size cells used in the asynchronous transmission mode. The utilisation of compact, fixed-size cells has various benefits. Secondly, by using tiny cells, a high-priority cell may wait less in line if it comes somewhat later than a lower-priority cell that has already used a resource (e.g., the transmitter). Second, switching between fixed-size cells seems to be more effective, which is crucial for ATM's very high data rates [PARE88]. It is simpler to implement the switching process in hardware while using fixed-size cells.

Only at the user-network interface does the Generic Flow Control (GFC) field exist; it does not present in the internal network cell header. Thus, it can only be utilised at the local user-network interface to manage cell flow. The field might be used to help the client manage traffic flow for various service characteristics. In any event, the network's short-term overload situations are relieved via the GFC process [9]. Specifies that all terminals must be able to access their guaranteed capacity in order for the GFC mechanism to function. Both the variable-bit-rate (VBR) terminals with a guaranteed capacity element and all constant-bit-rate (CBR) terminals.

The information type in the information field is indicated by the Payload Type (PT) field. The interpretation of the PT bits. User information is indicated by the first bit having a value of 0. The third bit, known as the Service Data Unit (SDU) type bit, is a one-bit field that may be used to distinguish between two kinds of ATM SDUs connected to a connection. In this situation, the second bit indicates if congestion has been encountered. The 48-octet payload of the cell is referred to as the SDU. If the first bit of the Payload Type field has a value of 1, it means that this cell contains network administration or maintenance data. Using this signal, network-management cells may be added to a user's VCC without affecting the user's data. As a result, the PT field may provide information on inband control.

When there is congestion, the Cell Loss Priority (CLP) bit is utilised to direct the network. If a cell has a value of 0, it is considered to be of comparatively greater importance and should not be removed unless there are no other options. When a cell has a value of 1, it means that it might be discarded from the network. If the network is not crowded, the user may utilise this field to insert more cells (beyond the specified rate) into the network with a CLP of 1 and transport them to the destination. Every data cell that violates a contract on traffic parameters between the user and the network may have this field set to 1 by the network. In this instance, the setting switch is aware that the cell exceeds the agreed-upon traffic parameters, yet the switch is able to manage the cell. If congestion arises later on in the network, this cell has been designated for discard in favour of cells that are within agreed-upon traffic restrictions.

Uncontrolled transmission and controlled transmission are the two sets of methods employed when the UNI's equipment is set up to support the GFC mechanism. Every link is, in essence, marked as being either susceptible to flow control or not. One group of regulated connections (Group A) may be the default for those who are subject to flow control, or controlled traffic may be divided into two groups of controlled connections (Group A and Group B); these are referred to, respectively, as the one-queue and two-queue models. The network side controls the flow of data in the direction from the subscriber to the network [10].

We start by thinking about how the GFC mechanism works when there is only one set of regulated connections. The controlled device, known as terminal equipment (TE), initialises two variables: GO CNTR, a credit counter, is set to 0, and TRANSMIT, a flag, is initialised to SET (1). At setup time, a third variable, GO VALUE, is either initialised to 1 or set to a bigger value. Cells on unsecured lines may be dispatched whenever they like. In the absence of cells, connections may be regulated or uncontrolled.If the controlling equipment sends out a HALT signal, TRANSMIT is set to 0 and stays there until a NO HALT signal arrives, at which point it is changed to 1.If none of the uncontrolled connections are available for cell transmission, then the TE is permitted to send a cell through a regulated connection. The TE decreases GO CNTR and indicates that cell as being on a regulated connection.When receiving a SET signal, the TE changes GO CNTR to GO VALUE; a null signal has no impact on GO CNTR.

The HALT signal should be cyclic and is used logically to restrict the actual ATM data rate. For instance, the HALT command is sent by the controlling equipment so that it is active 50% of the time to reduce the data rate over a link by half. Over the course of the physical connection's lifetime, this is done in a predictable, regular pattern. The data that are used as input in the calculation of the error code in the majority of existing protocols, such as HDLC, are typically much longer than the size of the resulting error code. This enables the detection of errors. In the case of ATM, the calculation's input is only 32 bits, as opposed to the code's 8 bits. The code can

sometimes be used for actual error correction in addition to error detection because the input is relatively short. This is due to the code having enough redundancy to recover from specific error patterns.

The HEC algorithm's operation at the receiver. The receiver's error correction algorithm is initially set to the single-bit error correction default mode. The HEC calculation and comparison are carried out as soon as each cell is received. The receiver stays in error correction mode as long as no errors are found. If a single-bit error is found, the receiver will fix it; if a multibit error is found, the receiver will recognise it. The receiver now enters detection mode in either scenario. There is no attempt to X8 + X2 + X + 1 in this mode.

This change was made in response to the realisation that a noise burst or other event could result in a series of errors for which the HEC is insufficient for error correction. As long as errored cells are received, the receiver is in detection mode. The receiver returns to correction mode once a header has been examined and determined to be error-free. The result of mistakes in the cell header is depicted in the flowchart. Under bursty error conditions, the error protection function offers recovery from single-bit header errors as well as a low probability of delivering cells with incorrect headers. Single-bit errors and relatively large burst errors appear to be a mix of the error characteristics of fiber-based transmission systems. The more time-consuming error correction capability may not be used for some transmission systems.

ATM cells can be transmitted using one of the following data rates: 622.08 Mbps, 155.52 Mbps, 51.84 Mbps, or 25.6 Mbps, according to I.432 specifications. The transmission structure that will be used to transport this payload must be specified. I.432 specifies two methods: a physical layer based on cells and another based on SDH. 2 We look at each of these strategies separately. Design parameters include and and their values. Longer synchronisation delays are caused by higher values of but the robustness against false delineation is increased. Longer detection lag times are caused by higher values of but the robustness against false misalignment is increased. The effect of random bit errors on cell delineation performance for different values of and. The first graph displays, with as a parameter, the typical amount of time that the receiver will keep synchronisation. The average time to acquire synchronisation is depicted in the function of error rate, with as a parameter.

When both the transmission and transfer mode functions are based on the same structure, a cell-based transmission scheme has the benefit of a more straightforward user interface. The ATM cell stream is given structure by the SDH-based physical layer. We examine the 1.432 specification for 155.52 Mbps in this section; comparable structures are utilised at other data rates. Framing is required for the SDH-based physical layer. The pointer in the section overhead of the frame suggests that this payload may be offset from the start of the frame. As can be seen, the payload is made up of an ATM cell-containing portion and a 9-octet path overhead portion. A cell may cross a payload boundary because the payload capacity (2340 octets) is not an integer multiple of the cell length (53 octets). The sending side sets the H4 octet in the path overhead to denote the arrival of the following cell boundary. In other words, the H4 field value represents the number of octets to the first cell boundary that comes after the H4 octet.

It can be used to carry either ATM-based or STM-based (synchronous transfer mode) payloads, enabling the deployment of a high-capacity fiber-based transmission infrastructure for a variety of circuit-switched and dedicated applications and then a smooth migration to the support of ATM. For instance, a connection carrying constant-bit-rate video traffic may be mapped into a

separate, circuit-switchable payload envelope of the STM-1 signal. This could be more effective than switching between ATMs. Several ATM streams can be combined to create interfaces with higher bit rates than those supported by the ATM layer at a specific site using SDH synchronous multiplexing techniques. For instance, four separate ATM streams with bit rates of 155 Mbps (STM-1) each can be combined to create an interface with a bit rate of 622-Mbps (STM-4).

This configuration might be less expensive than using a single 622-Mbps ATM stream. For example, a user expects a flow of audio or video information to be presented in a continuous, smooth fashion. A lack of continuity or excessive loss results in significant loss of quality. Applications that involve interaction between people have tight constraints on delay. Typically, any delay above a few hundred milliseconds becomes noticeable and annoying. Accordingly, the demands in the ATM network for switching and delivery of real-time data are high. Constant Bit Rate (CBR) (CBR) The CBR service is perhaps the simplest service to define. It is used by applications that require a fixed data rate that is continuously available during the connection lifetime and a relatively tight upper bound on transfer delay. CBR is commonly used for uncompressed audio and video information.

The principal difference between applications appropriate for rt-VBR and those appropriate for CBR is that rt-VBR applications transmit at a rate that varies with time. Equivalently, a rt-VBR source can be characterized as somewhat burst. For example, the standard approach to video compression results in a sequence of image frames of varying sizes. Because real-time video requires a uniform frame transmission rate, the actual data rate varies. The rt-VBR service allows the network more flexibility than CBR. The network is able to statistically multiplex a number of connections over the same dedicated capacity and still provide the required service to each connection.

Non-real-time services are intended for applications that have bursty traffic characteristics and do not have tight constraints on delay and delay variation. Available Bit Rate (ABR) (ABR) Bursty applications that use a reliable end-to-end protocol such as TCP can detect congestion in a network by means of increased roundtrip delays and packet discarding. This is discussed in Chapter 20. However, TCP has no mechanism for causing the resources within the network to be shared fairly among many TCP connections. Further,TCP does not minimise congestion as efficiently as is possible using explicit information from congested nodes within the network.

Guaranteed Frame Rate (GFR) (GFR) The most recent addition to the set of ATM service categories is GFR, which is designed specifically to support IP backbone subnetworks. GFR provides better service than UBR for frame-based traffic, including IP and Ethernet. A major goal of GFR is to optimise the handling of frame-based traffic that passes from a LAN through a router onto an ATM backbone network. Such ATM networks are increasingly being used in large enterprise, carrier, and Internet service provider networks to consolidate and extend IP services over the wide area. While ABR is also an ATM service meant to provide a greater measure of guaranteed packet performance over ATM backbones, ABR is relatively difficult to implement between routers over an ATM network. With the increased emphasis on using ATM to support IP-based traffic, especially traffic that originates on Ethernet LANs, GFR may offer the most attractive alternative for providing ATM service.

One of the techniques used by GFR to provide improved performance compared to UBR is to require that network elements be aware of frame or packet boundaries. Thus, when congestion requires the discard of cells, network elements must discard all of the cells that comprise a single

frame. GFR also allows a user to reserve capacity for each GFR VC. The user is guaranteed that this minimum capacity will be supported[11]. Additional frames may be transmitted if the network is not congested. Asynchronous Transfer Mode, is a telecommunications technology that has been widely used in the past for transmitting digital data, voice, and video information. Although it is no longer as popular as it used to be, it is still important to understand the basics of ATM and how it works. In this article, we will discuss ATM in 200 lines.

1. ATM was first introduced in the late 1980s as a way to improve the efficiency of telecommunications networks.
2. Unlike other networking technologies, such as Ethernet, ATM uses fixed-sized cells to transmit data.
3. Each ATM cell is 53 bytes long, consisting of a 5-byte header and a 48-byte payload.
4. The ATM header contains information about the source and destination of the cell, as well as other control information.
5. The payload of the ATM cell contains the actual data being transmitted.
6. ATM uses virtual circuits to transmit data between devices. A virtual circuit is a logical path that is established between two devices for the duration of a communication session.
7. Virtual circuits are established through a process called signaling, which is performed by a protocol called the ATM User-Network Interface (UNI).
8. The ATM UNI is responsible for establishing and maintaining virtual circuits, as well as exchanging data between devices.
9. In addition to the UNI, there is also an ATM Network-Network Interface (NNI), which is used to connect different ATM networks together.
10. ATM supports both point-to-point and multipoint connections. Point-to-point connections are established between two devices, while multipoint connections are established between one device and multiple devices.
11. ATM supports multiple quality of service (QoS) levels, which can be used to prioritize different types of traffic on the network.
12. ATM supports three different QoS classes: constant bit rate (CBR), variable bit rate (VBR), and available bit rate (ABR).
13. CBR is used for real-time applications, such as voice and video, which require a fixed amount of bandwidth.
14. VBR is used for applications, such as video streaming, which require a variable amount of bandwidth.
15. ABR is used for applications, such as file transfers, which do not require a guaranteed amount of bandwidth but can benefit from additional bandwidth when it is available.

16. ATM uses a technique called cell switching to transmit data between devices. Cell switching involves breaking up the data into small, fixed-size cells and transmitting them individually.

17. Each ATM cell is transmitted independently, which allows multiple cells to be transmitted simultaneously.

18. Cell switching allows ATM to provide high-speed, low-latency communication, which is especially important for real-time applications.

19. ATM is capable of transmitting data at speeds of up to 622 Mbps over a single connection.

20. ATM is typically used in conjunction with other networking technologies, such as SONET/SDH, to create high-speed, reliable communication networks.

21. SONET/SDH provides the physical layer for the network, while ATM provides the data layer.

22. ATM can be used to transmit a wide range of data types, including voice, video, and data.

23. Voice and video data are typically transmitted using a technique called packetization, which involves breaking up the data into smaller packets and transmitting them using ATM.

24. Data is typically transmitted using a technique called segmentation and reassembly (SAR), which involves breaking up the data into smaller segments and transmitting them using ATM.

25. ATM supports several different types of connections, including permanent virtual circuits (PVCs) and switched virtual circuits (SVCs).

26. PVCs are established in advance and provide a dedicated, fixed path for data transmission.

CONCLUSION

ATM's impact on the development of high-speed networking technologies cannot be underestimated. Although it has been largely replaced by newer technologies, its legacy can still be seen in modern data communication networks. As the world continues to evolve and the demand for high-speed data transmission increases, it is essential to continue developing and improving data communication technologies to meet the ever-growing demands of the modern world.

REFERENCES

[1] J. P. Coudreuse, G. Pays, and M. Trouvat, “Asynchronous transfer mode,” *Commut. Transm.*, 1990, doi: 10.1201/b15844-12.

[2] J. Y. Le Boudec, “The Asynchronous Transfer Mode: a tutorial,” *Computer Networks and ISDN Systems*. 1992. doi: 10.1016/0169-7552(92)90114-6.

[3] M. I. Goulamghoss and V. Bassoo, “Analysis of traffic engineering and fast reroute on multiprotocol label switching,” *J. Ambient Intell. Humaniz. Comput.*, 2021, doi: 10.1007/s12652-020-02365-5.

[4] S. Al-Sharhan, F. Karray, and W. Gueaieb, “Learning-based resource optimization in asynchronous transfer mode (ATM) networks,” *IEEE Trans. Syst. Man, Cybern. Part B Cybern.*, 2003, doi: 10.1109/TSMCB.2003.808178.

[5] G. Niestegge, “The ‘leaky bucket’ policing method in the ATM (asynchronous transfer mode) network,” *Int. J. Digit. Analog Commun. Syst.*, 1990, doi: 10.1002/dac.4510030214.

[6] I. A. Ibrahim Diyeb and S. A. Alhomdy, “Frame Relay versus Asynchronous Transfer Mode: A Comparative Study and Simulation,” *Int. J. Comput. Netw. Inf. Secur.*, 2017, doi: 10.5815/ijcnis.2017.10.04.

[7] J. F. Heautot *et al.*, “Influence of the teleradiology technology (N-ISDN and ATM) on the inter-hospital management of neurosurgical patients,” *Med. Inform. Internet Med.*, 1999, doi: 10.1080/146392399298465.

[8] H. K. Huang, R. L. Arenson, W. P. Dillon, S. L. Lou, T. Bazzill, and A. W. K. Wong, “Asynchronous transfer mode technology for radiologic image communication,” *Am. J. Roentgenol.*, 1995, doi: 10.2214/ajr.164.6.7754909.

[9] I. A. Hieder, S. M. Abdullah, and R. A. Ali, “Utilizing the ATM technology in E-distance learning,” *Indones. J. Electr. Eng. Comput. Sci.*, 2020, doi: 10.11591/ijeecs.v20.i2.pp1016-1029.

[10] R. Noro, J. P. Hubaux, R. Meuli, R. N. Laurini, and R. Patthey, “Real-time telediagnosis of radiological images through an asynchronous transfer mode network: The ARTeMeD project,” *J. Digit. Imaging*, 1997, doi: 10.1007/bf03168673.

[11] S. Rajagopalan, “A study on mpls vs sd-wan,” *Lect. Notes Data Eng. Commun. Technol.*, 2021, doi: 10.1007/978-981-16-0965-7_25.

CHAPTER 24

EFFICIENT ROUTING STRATEGIES FOR SWITCHED NETWORKS: A COMPARATIVE STUDY OF TRADITIONAL AND MODERN APPROACHES

Pankaj Kumar Goswami, Associate Professor
Department of Electronics and Communication Engineering,
Teerthanker Mahaveer University, Moradabad, Uttar Pradesh, India
Email Id- g.pankaj1@gmail.com

ABSTRACT:

Routing in switched networks is an important aspect of data communication that involves directing data packets from their source to their destination through a series of interconnected switches. The goal of routing is to ensure that data packets are delivered efficiently and reliably, while minimizing delays and congestion. Switched networks use different routing protocols, such as Spanning Tree Protocol (STP), Open Shortest Path First (OSPF), and Border Gateway Protocol (BGP), to determine the most efficient path for data packets to travel. These routing protocols use different algorithms to calculate the optimal path based on factors such as the network topology, traffic load, and link availability.

KEYWORDS:

Data Network, Gateway Protocol, Network Topology, Spanning Tree, Shortest Path.

INTRODUCTION

Routing in switched networks refers to the process of forwarding data packets from one network device to another through a series of interconnected switches. In switched networks, each network device is typically connected to a switch, which acts as a central hub for forwarding packets to their intended destination. When a device sends a packet, the switch examines the packet's destination address and uses its routing table to determine the best path to forward the packet. The routing table contains information about the network topology, including the addresses of other switches and the devices that are connected to them [1]–[3] .

Switched networks can use various routing protocols, such as Spanning Tree Protocol (STP), Open Shortest Path First (OSPF), and Routing Information Protocol (RIP), to ensure that packets are forwarded efficiently and quickly. These protocols allow switches to exchange information about the network topology and make decisions about the best path to forward packets based on factors such as distance, bandwidth, and link quality. Overall, routing in switched networks is critical to ensure that data packets are delivered quickly and reliably to their intended destination, enabling efficient communication and information sharing across the network. Routing in switched networks involves the process of forwarding data packets between different network devices. Switched networks are a type of computer network that uses switches to connect network devices and enable communication between them [4] .

In a switched network, each device is connected to a switch, which is responsible for directing data packets to their destination. The switch maintains a table of MAC addresses, which are used to identify the network devices. When a packet is received at a switch, the switch examines the packet's destination MAC address and forwards the packet to the appropriate port leading to the destination device. Routing in switched networks can be either static or dynamic. Static routing involves manually configuring the routes in the network. This is typically done in small networks with few devices. Dynamic routing, on the other hand, involves using routing protocols to dynamically determine the best path for data packets. This is more commonly used in larger networks, as it allows for automatic adaptation to changes in the network topology.

Common routing protocols used in switched networks include the Routing Information Protocol (RIP), Open Shortest Path First (OSPF), and Border Gateway Protocol (BGP). These protocols enable the switches in the network to communicate with each other and exchange routing information, allowing for efficient packet forwarding and network optimization [5]. In switched networks, routing can occur at both layer 2 and layer 3 of the OSI model. Layer 2 switching, also known as switching based on MAC addresses, is used to forward packets within a local area network (LAN). In this type of switching, each switch maintains a table of MAC addresses, known as the MAC address table, which it uses to determine the destination of incoming packets.

Layer 3 switching, also known as routing based on IP addresses, is used to forward packets between different subnets or networks. In this type of switching, the switch looks at the packet's destination IP address and uses routing protocols to determine the best path to forward the packet to its destination. One important aspect of routing in switched networks is the concept of VLANs (Virtual Local Area Networks). VLANs are used to segment a network into multiple virtual networks, each with its own broadcast domain. This allows for better network management, improved security, and more efficient use of network resources. In a switched network with VLANs, routing is used to forward packets between VLANs, allowing communication between devices on different VLANs.

To summarize, routing in switched networks involves the forwarding of data packets between network devices, typically using switches. Routing can occur at layer 2 or layer 3 of the OSI model, and can be either static or dynamic. Routing protocols are used to determine the best path for data packets, and VLANs are used to segment a network into multiple virtual networks. For packet-switching, frame-relay, ATM, as well as for the Internet and internetworks, several routing algorithms have been devised. There are many common ideas among these algorithms. Routing systems may be grouped based on a variety of criteria, including such is the criteria used to choose the optimal path between two nodes, the method used to gather the information required to choose the path, and whether a distributed or centralised algorithm is employed.

The routing function searches the network for the least-cost path, where cost is determined by the number of hops, the anticipated latency, or other factors. Algorithms for adaptive routing often depend on nodes exchanging data about traffic conditions. Routing is a crucial design consideration for switched networks, including packet-switching, frame relay, ATM, and internets. The routing function, in general, aims to create routes across the network for certain pairs of communicating end nodes so that the network is used effectively.

An overview of the problems with route design is provided at the beginning of this chapter. We next discuss least-cost algorithms, which are a crucial component of routing in switched networks, before turning our attention to the routing function in packet-switching networks. Both

packet-switching networks and routing in internets are addressed by these subjects. Routing is one of the trickiest and most important architectural elements of switched data networks.

DISCUSSION

The most typical definition, which we employ, is that the number of connections between network nodes (such as packet-switching nodes, ATM switches, routers, etc.) that a packet traverses along that journey constitutes the number of hops along a path from a given source to a given destination. The links between the source station and the network and the destination station and the network are sometimes included in the definition of the hop count. The value obtained by the latter definition is two more than the value obtained by our definition [6], [7].

Accepting packets from a source station and sending them to a destination station is the main duty of a packet-switching network. A path or route across the network must be chosen in order to do this; often, more than one route is viable. Thus, a routing operation must be carried out. Correctness, fairness, simplicity, optimality, robustness, efficiency, and stability are necessary for this function. Correctness and simplicity, the first two elements on the list, go without saying. The ability of the network to send packets over a particular route in the face of localised failures and overloads is referred to as robustness.

The network should be able to respond to such events without losing packets or destroying virtual circuits. The opposing necessity for stability must be managed by the designer who desires robustness. Methods that adapt to shifting circumstances unfortunately have a propensity to either respond to events too slowly or undergo unsteady swings from one extreme to another. By moving the majority of the load to a second location, for instance, the network may respond to congestion in one area. A second shift is now necessary since the second area is now congested and the first is underused. Packets may go in circles through the network during these transitions.

Also, there is a trade-off between justice and efficiency. The exchange of packets between adjacent stations may be given a greater priority by certain performance criteria than an exchange between stations that are further apart. While this approach could increase average throughput, it will look unfair to the station that has to connect with other stations in the distance the most. Lastly, each routing method reduces network efficiency by adding processing cost at each node and often by adding transmission overhead as well [8]. Such overhead must have a cost that is smaller than the gain realised based on some credible criteria, such as improved fairness or robustness. Several of these classifications cross across or are interdependent. Yet, a review of this list helps to organise and explain routing ideas. Performance Standards a performance criteria is often used to choose which route to take. The simplest criteria is to choose the network path with the fewest number of nodes that it travels through, or the minimum-hop path. 1 This criteria is simple to assess and ought to use the least amount of network resources. Least-cost routing is an extension of the minimum-hop criteria.

Network configuration, each connection has a cost connected to it, and for every pair of linked stations, the least expensive path across the network is attempted a network where a connection between two nodes is represented by two arrowed lines, and the accompanying numbers show the current link cost in each direction. The least expensive route is 1-4-5-6, however the shortest path (fewest hops) from node 1 to node 6 is 1-3-6. Links have costs allocated to them in order to serve one or more design goals. Examples include the present queuing time on the connection or

the data rate (i.e., the greater the data rate on a link, the lower the ascribed cost of the link). The least expensive route ought to provide the most throughput in the first scenario. The second scenario should have the least amount of delay possible.

The optimal route for every pair of stations may be found using either the minimum-hop or least-cost strategy, and both computations would take about the same amount of time to complete. The least-cost criteria is more often used than the minimum-hop criterion because it is more forgiving. Decision Time and Location Several performance criteria are used to guide routing choices. The decision's timing and location are two of its most important attributes.

Whether a routing choice is made based on a packet or a virtual circuit affects the decision time. A routing choice is made for each packet when the network operates internally as a datagram. A routing choice is made at the moment the virtual circuit is constructed for internal virtual circuit functioning. In the simplest scenario, the path taken by each successive packet utilising that virtual circuit is the same. With more advanced network architectures, the network may alter the route allocated to a specific virtual circuit dynamically in response to changing circumstances (e.g., overload or failure of a portion of the network).

The phrase "decision place" describes which network node or nodes are in charge of making the routing choice. Distributed routing is the most typical kind, where each node is in charge of choosing an output connection to route packets as they come in. With centralised routing, a specified node, such as a network control centre, makes the choice. This latter strategy runs the risk of preventing network functioning if the network control centre is lost. While the distributed strategy may be more sophisticated, it is also more reliable. Source routing is a third option that some networks adopt. In this instance, the source station rather than a network node actually decides on the routing and transmits that choice to the network. This enables the user to specify a path over the network that satisfies personal requirements [9].

Decision location and timing are separate design factors. Assume, for instance, that each node in the decision point and that the numbers shown represent the costs at a certain point in time; the costs may fluctuate. If a packet has to go from node 1 to node 6, it may take the path 1-4-5-6, with the transmitting node choosing each leg of the route locally. Now let's modify the variables such that 1-4-5-6 is no longer the best course. The next packet in a datagram network could take a different path, which is again decided by each node along the way. Each node in a virtual circuit network will retain the routing choice made when the virtual circuit was created, and will simply forward the packets without making a new choice.

Source of Network Information and Time of Update The majority of routing systems demand that choices be made in light of the network structure, traffic volume, and connection cost. Strangely, some tactics don't utilise this information and nevertheless succeed in sending packets; examples of these tactics include flooding and a few random tactics which will be described later. Each nodes may only utilise local information, such as the cost of each outgoing connection, in distributed routing, where the routing decision is determined by each node. Each node may also gather data from nearby nodes, such as the degree of congestion present there. The node may get information from all nodes along any conceivable path of interest thanks to techniques that are widely used. When routing is centralised, the central node often uses data collected from all nodes.

Timing of information updates, which depends on both the information source and the routing mechanism, is a similar idea. It is obvious that there won't be any information to update if no information is utilised as in floods. The update is nearly continuous if just local data is utilised. In other words, each node is aware of its surroundings at all times. Update time for nearby nodes and all other information source types is determined by the routing method. The data is never updated for a fixed approach. Information is periodically updated for an adaptive method so that the routing choice may adjust to changing circumstances.

As one would anticipate, the more information that is provided and updated regularly, the more probable it is that the network will make wise routing choices. Nevertheless, sending such information requires resources from the network. To address the routing needs of packet-switching networks, several routing algorithms have developed. Fixing the Route each source-destination pair of nodes in the network is set with a single, permanent route for fixed routing. You might use one of the least-cost routing techniques. The routes are set, or at the very least, they only change when the network topology does. Hence, no dynamic variable, such as traffic, may be predicated on the connection costs employed in route planning. Nonetheless, they could be determined by capacity or anticipated traffic. There is a creation of a central routing matrix, which may be kept in a network control centre. The matrix displays the next node along the path for each source-destination pair of nodes.

Keep in mind that not every feasible pair of nodes requires the storage of the whole route. Instead, knowing the initial node on the path for each pair of nodes is sufficient. Assume that the X-A connection is the starting point of the least-cost path from X to Y to illustrate how this works. This is the section of the route that goes from A to Y. What is the cheapest way to go from A to Y? The X-Y route may be improved by using instead if the cost of is higher than that of. Therefore, As a result, just the identification of the next node, and not the whole path, is required at each point along a route. In this example, the first node through which the path from node 1 to node 6 passes is node 4. Using the matrix once again, node 5 is the connection point between nodes 4 and 6. Last but not least, the connection from node 5 to node 6 is a straight one. The whole circuit from node 1 to node 6 is thus 1-4-5-6.

There is a minimum-hop route for every pair of connected end systems. The diameter of the network is equal to the length of the longest such minimum-hop route towards nodes 3 and 4. Nodes 2, 3, and 5 will get a copy from Node 4. Thus it continues. The packet will eventually arrive in several copies at node 6. In order for node 6 to know to only save the first copy, the packet has to carry some kind of distinctive identification for example, the source node and sequence number, or virtual circuit number and sequence number.

The number of packets in circulation only from a single source packet increases without limit unless something is done to halt the constant retransmission of packets. Each node should keep track of the names of the packets it has previously retransmitted in order to avoid this, for example. Duplicate copies of the package are discarded as they come in. A hop count field that is included with each packet is a simpler method. The diameter of the network the length of the longest minimum-hop route across it 2 may be used as the initial number for the count.

A packet with a hop count of 3 is intended to be forwarded from node 1 to node 6. Three copies of the packet are made on the first hop, reducing the hop count to two. There are nine copies produced for the second hop of all these copies. Node 6 receives one of these copies and realises it is the intended recipient. As a result, it does not retransmit. On their third and final hop, the

other nodes create a total of 22 new copies. Be aware that a node may create several copies at this third step if it is not tracking the packet identification. Due to the exhaustion of the hop count, all packets received from the third hop are rejected. Node 6 has now received a total of four extra copies of the packet.

The flooding approach is quite strong and might be used to deliver emergency messages because of the first attribute. One use case is a military network that is vulnerable to severe destruction. Flooding could be utilised initially to build up the path for a virtual circuit due to the second feature. We shall see that flooding is utilised in various systems to broadcast routing information. The third feature implies that flooding might be effective for the distribution of crucial information to all nodes.

Random Direction With far less traffic demand, random routing provides the same simplicity and resilience as flooding. A node only chooses one outgoing route when using random routing to retransmit an incoming packet. With the exception of the connection on which the packet arrived, the outgoing link is selected at random. If every connection has an equal chance of being picked, a node may just use outgoing links in a round-robin method. If the probability is determined by data rate, then we have where the total is divided across all potential outgoing connections. This plan ought to provide a balanced allocation of traffic. Be aware that fixed network costs might potentially form the basis of the probability.

Random routing necessitates the usage of no network information, similar to flooding. The real route usually isn't the least expensive or the shortest path since it is chosen at random. As a result, while not quite as high as for floods, the network must bear a larger than optimal traffic load. Intelligent Routing An adaptive routing method is utilised in almost all packet-switching networks. In other words, when network circumstances change, so do the routing choices that are made. Failure: A node or connection that fails cannot be utilised as part of a route. This is one of the main factors that affect routing choices. The level of information quality and the quantity of overhead must be balanced in this situation. The routing choices made by each node will be better the more information that is shared and the more often it is exchanged. An adaptive method may respond too rapidly, generating congestion-producing oscillation, or too slowly, becoming irrelevant. On the other hand, this information is itself a strain on the component networks, causing a performance deterioration.

Adaptive routing techniques are by far the most used notwithstanding these genuine risks for two reasons: Depending on the soundness of the design and the kind of the load, these advantages may or may not be achieved. Generally speaking, adaptive routing is a very difficult operation to do well. As evidence of this, the majority of significant packet-switching networks, including the ARPANET and its offspring as well as many commercial networks, have undergone at least one significant revision to their routing protocol. A node directing every packet to the outgoing connection with the least queue length, Q, is an example of an adaptive routing technique that solely uses local data. The strain on outgoing connections would be balanced as a result of this. Certain outgoing connections, nevertheless, may not be pointing in the right general direction. By adding considering desired direction, much as with random routing, we can make things better. For each destination I each connection leaving the node in this scenario would have a bias, with lower values of indicating more favoured paths. The node would choose the outgoing connection with the lowest overhead for each incoming packet destined for node i.

Since they do not take use of readily accessible information, adaptive methods that exclusively employ local information are seldom deployed. It is usual to find strategies that use data from nearby nodes or from every node. Both benefit from the knowledge each node has about the delays and disruptions it encounters. Distributed or centralised adaptive techniques are both viable options. Each node shares delay information with other nodes in the distributed situation. A node uses a least-cost routing algorithm to determine the latency situation throughout the network based on the information it receives. In the centralised scenario, each node notifies the central node of its connection delay status, and the central node creates routes based on this input before sending the routing data back to the nodes.

We examine a number of routing strategy examples in this section. All of them were first created for the packet-switching network known as ARPANET, which served as the ancestor of the modern Internet. For a number of reasons, analysing these tactics is instructive. Secondly, many packet-switching networks, including several networks on the Internet, use these and related technologies. Second, both the Internet and commercial internetworks have implemented routing protocols based on the ARPANET work. And lastly, the way the ARPANET routing system developed sheds light on some of the major design difficulties surrounding routing algorithms.

The first routing method was developed in 1969 and used a distributed adaptive algorithm with a modified Bellman-Ford algorithm as the performance criteria. Each node in this method stores two vectors, where sij denotes the node after it along the current minimum-delay path from I to j. Si is the successor node vector for node I N is the total number of nodes in the network, and dij is the current estimate of the minimal delay between node I and node j (1dii = 02). Di is the delay vector for node I and Si is the successor node vector for node i. Each node exchanges its delay vector with each of its neighbours once every 128 milliseconds. A node k updates both of its vectors in the manner described below based on all incoming delay vectors: The initial routing algorithm was changed in 1979 by a quite different one after several years of use and a few minor tweaks [MCQU80]. The following were the main flaws in the prior algorithm: It only took wait length into account and ignored line speed. As a result, linkages with greater capacity did not get the favourable treatment they merited.

In any event, queue length is a fictitious indicator of delay since there is always some processing time between a packet's arrival at a node and its entry into an outbound queue. The algorithm wasn't very precise. In particular, it took a while to react as delays and congestion worsened. The new method also uses latency as the performance criteria and is distributed adaptive, but there are several key modifications. The delay is measured directly, as opposed to utilising queue length as a proxy for it. Every packet that arrives at a node is timestamped with an arrival time. When the packet is transferred, a departure time is noted. The delay for a packet is calculated as the departure time minus the arrival time plus transmission time and propagation delay if a positive acknowledgement is given. Hence, the node must be aware of the propagation time and connection data rate. The departure time is adjusted in the event of a negative acknowledgement, and the node attempts again until a successful transmission delay is determined.

Flooding is used to distribute the information to all other nodes if the latency varies significantly. Every node keeps track of an estimate of each network link's latency. Third Generation recalculates its routing table using Dijkstra's algorithm whenever fresh information is received. Experience with this new approach showed that it was more reliable and responsive than the previous one. Since each node only performs this activity once per 10 seconds at most, the

overhead caused by flooding was modest. The new technique did have certain drawbacks, however, and was changed in 1987 as the network's load increased and the flaws became more apparent.

The issue with the second technique is that it makes the erroneous assumption that a connection's measured packet delay is a reliable indicator of the link delay that will be experienced when all nodes have rerouted their traffic in accordance with this reported delay. As a result, it only serves as a useful routing method if there is some relationship between the reported values and the values that are actually experienced after rerouting. For modest and moderate traffic volumes, this correlation is often very strong. Under large weights, there isn't much of a link. The routing tables are thus no longer valid as soon as all nodes have updated their routing information!

Consider a network with two areas and just two connections, A and B, linking the two regions as an example. One of these connections must be traversed on every path between two nodes located in distinct areas. Imagine that link an experiences a significant increase in traffic. The connection delay on node A will be significantly increased as a result, and all other nodes will be informed of this delay value at the earliest opportunity. All nodes will get these changes at around the same time, and each will promptly update its routing tables. This new link A delay value is probably going to be large enough to make link B the preferable option for the most, if not all, interregion trips. As every node modifies its routes simultaneously, connection B receives the majority of interregional traffic at the same time. There will then be a shift to connection A as the link delay value on B increases at this point. This oscillation won't stop until the amount of traffic decreases.

Designers of the ARPANET came to the conclusion that the fundamental cause of the issue was that every node was attempting to find the optimal path to every destination, and that these attempts were in conflict. It was determined that under large loads, routing should focus on providing a decent path for the average route rather than trying to provide the optimal path for every route. The creators opted against altering the routing algorithm as a whole. Instead, changing the function that determines connection costs was sufficient. In order to dampen routing oscillations and lower routing overhead, this was done. The average delay over the last 10 seconds is first calculated. The following processes are then used to modify this value:

An estimate of link usage is created from the observed delay using a simple single-server queuing model. Utilization may be represented as a function of delay as follows, according to queuing theory: The network-wide average packet size (600 bits) divided by the link's data rate was used to determine the service time.Next, the result is smoothed by averaging it with the prior utilisation estimate: where Averaging lengthens the time of routing oscillations and lowers routing overhead.Next, the connection cost is established as a function of average use, which is intended to provide a reliable cost estimate without fluctuation. The process of converting the estimated usage estimate into a cost value In essence, the ultimate cost value is the changed value of the delay.

The lowest value up to a certain level of usage is attained. At low traffic volumes, this feature has the effect of lowering routing overhead. The cost level is permitted to increase up to a maximum value that is three times the minimum value if usage reaches a particular point. This maximum setting has the effect of forbidding traffic from being routed over more than two extra hops in order to avoid a frequently used line. Be aware that the minimum requirement for satellite connections is greater. Since terrestrial lines have substantially smaller propagation

delays than wireless ones, this promotes their usage when there is less traffic. Furthermore take note of the fact that, at high utilisation levels, the real delay curve is substantially steeper than the transformation curves. All of the traffic on a connection is shed as a result of this sharp increase in link cost, which in turn leads to oscillations in routing [10].

Determine the shortest pathways from a given source node to all other nodes by building the paths in decreasing order of path length, according to Dijkstra's algorithm. The algorithm develops gradually. At the kth step, the shortest routes to the k nodes that are in a set T and least expensively far from the source node have been identified. The node outside of T that has the shortest route to the source node is added to T at this step. Each node's route from the source is specified when it is added to T.

CONCLUSION

Routing in switched networks plays a critical role in ensuring the efficient and reliable transmission of data, making it a key consideration in the design and implementation of data communication networks. As the demand for high-speed data transmission continues to grow, it is important to continue developing and improving routing protocols to meet the evolving needs of modern networks [11]. The efficiency and reliability of routing protocols directly impact the user experience and the ability of organizations to achieve their business objectives through technology. Therefore, it is essential to choose the appropriate routing protocols and continually monitor and optimize them to ensure the best performance for the network.

REFERENCES

[1] M. A. Bayir and M. Demirbas, “On the fly learning of mobility profiles for routing in pocket switched networks,” *Ad Hoc Networks*, 2014, doi: 10.1016/j.adhoc.2013.11.011.

[2] L. Li, Y. Zhang, W. Chen, S. K. Bose, M. Zukerman, and G. Shen, “Naïve Bayes classifier-assisted least loaded routing for circuit-switched networks,” *IEEE Access*, 2019, doi: 10.1109/ACCESS.2019.2892063.

[3] S. Wang, M. Liu, X. Cheng, and M. Song, “Routing in pocket switched networks,” *IEEE Wirel. Commun.*, 2012, doi: 10.1109/MWC.2012.6155878.

[4] T. E. Amah, M. Kamat, W. Moreira, K. Abu Bakar, S. Mandala, and M. A. Batista, “Towards next-generation routing protocols for pocket switched networks,” *Journal of Network and Computer Applications*. 2016. doi: 10.1016/j.jnca.2016.05.011.

[5] Y. Lee and J. M. Tien, “Static and dynamic approaches to modeling end-to-end routing in circuit-switched networks,” *IEEE/ACM Trans. Netw.*, 2002, doi: 10.1109/ TNET.2002.803909.

[6] R. R. Sarkar, K. Rasul, and A. Chakrabarty, “Survey on Routing in Pocket Switched Network,” *Wirel. Sens. Netw.*, 2015, doi: 10.4236/wsn.2015.79010.

[7] C. Sun, W. Guo, Z. Liu, M. Xia, and W. Hu, “Performance analysis of storage-based routing for circuit-switched networks,” *J. Opt. Commun. Netw.*, 2016, doi: 10.1364/ JOCN.8.000282.

[8] C. Yahaya, M. S. Abd Latiff, and A. B. Mohamed, “A review of routing strategies for optical burst switched networks,” *Int. J. Commun. Syst.*, 2013, doi: 10.1002/dac.1345.

[9] C. F. Hsu, T. L. Liu, and N. F. Huang, "Performance analysis of deflection routing in optical burst-switched networks," *Proc. - IEEE INFOCOM*, 2002, doi: 10.1109/INFCOM.2002.1019247.

[10] J. X. Cao, G. J. Chen, J. Yang, Z. Q. Zhu, and B. Liu, "Social-based routing in pocket switched networks," *Tongxin Xuebao/Journal Commun.*, 2015, doi: 10.11959/j.issn.1000-436x.2015105.

[11] D. G. Cantor and M. Gerla, "Optimal Routing in a Packet-Switched Computer Network," *IEEE Trans. Comput.*, 1974, doi: 10.1109/T-C.1974.223806.